MES-2110

Intelligent Layer 2 Switch

User's Guide

Default Login Details

IP Address	http://192.168.1.1
User Name	admin
Password	1234

Firmware Version 1.00
Edition 2, 9/2009

ZyXEL

www.zyxel.com

Copyright © 2009
ZyXEL Communications Corporation

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the Switch using the web configurator.

Related Documentation

- Command Line Interface (CLI) Reference Guide

  Line commands offer an alternative to the web configurator and in some cases are necessary to configure advanced features.

Note: It is recommended you use the web configurator to configure the Switch.

- Support Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.

- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

> **Warnings tell you about things that could harm you or your device.**

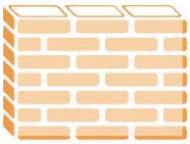
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The MES-2110 may be referred to as the "Switch", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The Switch icon is not an exact representation of your device.

The Switch	Computer	Notebook computer
Server	DSLAM	Firewall 
Telephone	Router	

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Do not obstruct the device ventillation slots as insufficient airflow may harm your device.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Use ONLY power wires of the appropriate wire gauge (see Chapter 22 on page 165 for details) for your device. Connect it to a power supply of the correct voltage (see Chapter 22 on page 165 for details).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- The length of exposed (bare) power wire should not exceed 7 mm.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Contents Overview

Introduction and Hardware 17

Getting to Know Your Switch 19
Hardware Installation and Connection 25
Hardware Overview 29

Basic Configuration 35

The Web Configurator 37
System Details 47

Configuration 51

Configuration 53
Loop Detection 59
Jumbo Frame 63
802.1x 65
Bridge 75
VLAN 83
Bandwidth Control 95
Broadcast Storm Control 97
Port Mirroring 99
Link Aggregation 101
IGMP 107
IP Source Guard 119
MAC 127
QoS 135

Management 143

Mgmt Config and System Restart Menu 145

Troubleshooting & Product Specifications 159

Troubleshooting 161
Product Specifications 165

Appendices and Index 169

Table of Contents

About This User's Guide **3**

Document Conventions **5**

Safety Warnings **7**

Contents Overview **9**

Table of Contents **11**

Part I: Introduction and Hardware **17**

Chapter 1
Getting to Know Your Switch **19**

1.1 Introduction 19
1.1.1 Backbone Application 19
1.1.2 Bridging Example 20
1.1.3 High Performance Switching Example 21
1.1.4 IEEE 802.1Q VLAN Application Examples 21
1.1.5 Metro Ethernet 22
1.2 Ways to Manage the Switch 23
1.3 Good Habits for Managing the Switch 23

Chapter 2
Hardware Installation and Connection **25**

2.1 Installation Scenarios 25
2.2 Desktop Installation Procedure 25
2.3 Mounting the Switch on a Rack 26
2.3.1 Rack-mounted Installation Requirements 26
2.3.2 Attaching the Mounting Brackets to the Switch 27
2.3.3 Mounting the Switch on a Rack 28

Chapter 3
Hardware Overview **29**

3.1 Front Panel 29
3.1.1 Console Port 30
3.1.2 Gigabit Ethernet Ports 30
3.1.3 Mini-GBIC Slots 31

3.1.4 Power Connector 33
3.2 LEDs 34

Part II: Basic Configuration 35

Chapter 4
The Web Configurator 37

4.1 Introduction 37
4.2 System Login 37
4.3 The Main Screen 39
4.3.1 Set Up the Administrative Password 44
4.4 Saving Your Configuration 44
4.5 Switch Lockout 45
4.6 Resetting the Switch 45
4.6.1 Reload the Configuration File 45

Chapter 5
System Details 47

5.1 Overview 47
5.2 The System Information Screen 47
5.3 The Board Information Screen 48
5.4 The DHCP Configuration Screen 49

Part III: Configuration 51

Chapter 6
Configuration 53

6.1 Overview 53
6.2 The Port Configuration Screen 53
6.3 The Port Status Screen 55
6.4 The RMON Status Screen 57

Chapter 7
Loop Detection 59

7.1 Overview 59
7.2 The Loop Detection Screen 60

Chapter 8
Jumbo Frame 63

8.1 Overview 63

8.2 The Jumbo Frame Configuration Screen 63

Chapter 9
802.1x 65

9.1 Overview 65
9.1.1 IEEE 802.1x Authentication 65
9.1.2 Guest VLAN 66
9.2 802.1x Global Configuration Screen 67
9.3 802.1x Radius Server Configuration Screen 67
9.4 802.1x Port Configuration Screen 68
9.5 802.1x Radius Server Configuration Screen 70
9.6 Technical Reference 71
9.6.1 RADIUS and TACACS+ 71
9.6.2 Supported RADIUS Attributes 71
9.6.3 Attributes Used for Authentication 72
9.6.4 Attributes Used for Accounting 73

Chapter 10
Bridge 75

10.1 Overview 75
10.1.1 STP Terminology 75
10.1.2 How STP Works 76
10.1.3 STP Port States 77
10.2 The Bridge Configuration Screen 77
10.3 The RSTP System Configuration Screen 78
10.4 The Spanning Tree Port Configuration 80

Chapter 11
VLAN 83

11.1 Overview 83
11.2 Introduction to IEEE 802.1Q Tagged VLANs 83
11.2.1 Forwarding Tagged and Untagged Frames 84
11.3 The VLAN Type Screen 85
11.4 The Port-Based VLAN Screen 85
11.5 The Tag-Based VLAN Screens 87
11.5.1 VLAN Stacking 87
11.5.2 VLAN Stacking Example 87
11.5.3 VLAN Stacking Port Roles 88
11.5.4 VLAN Tag Format 89
11.5.5 Frame Format 89
11.5.6 The VLAN Stacking Configuration Screen 90
11.5.7 The Tag-Based Port Information Screen 91
11.5.8 The Tag-Based Port Configuration Screen 93

11.5.9 The Management VLAN Screen 94

Chapter 12
Bandwidth Control 95

12.1 Overview 95
12.2 Bandwidth Control Setup 95

Chapter 13
Broadcast Storm Control 97

13.1 Overview 97
13.2 Broadcast Storm Control Setup 97

Chapter 14
Port Mirroring 99

14.1 Overview 99
14.2 Port Mirroring Setup 99

Chapter 15
Link Aggregation 101

15.1 Overview 101
15.2 Dynamic Link Aggregation 101
15.2.1 Link Aggregation ID 102
15.3 Static Trunking Example 102
15.4 Link Aggregation Setting 103
15.5 Link Aggregation Control Protocol 104
15.6 LACP Link Status 105

Chapter 16
IGMP 107

16.1 Overview 107
16.1.1 IP Multicast Addresses 107
16.1.2 IGMP Snooping 107
16.1.3 IGMP Snooping and VLANs 108
16.2 IGMP Configuration 108
16.3 IGMP Status 110
16.4 MVR Overview 110
16.4.1 Types of MVR Ports 111
16.4.2 MVR Modes 111
16.4.3 How MVR Works 111
16.5 General MVR Configuration 112
16.6 MVR Group Configuration 114
16.6.1 MVR Configuration Example 116

Chapter 17
IP Source Guard 119

17.1 Overview 119
17.1.1 DHCP Snooping Overview 119
17.2 DHCP Snooping Configuration 121
17.3 DHCP Binding Table 123
17.4 The ARP Inspection Screen 124
17.4.1 Configuring ARP Inspection 125

Chapter 18
MAC 127

18.1 Overview 127
18.2 The MAC Table Status Screen 128
18.3 The Lock MAC Address Learning Screen 129
18.4 The MAC Filter Configuration Screen 130
18.4.1 The MAC Filter Mode Screen 132
18.5 The MAC Limit Configuration Screen 133

Chapter 19
QoS 135

19.1 Overview 135
19.2 The QoS Base Configuration Screen 135
19.2.1 Configuring the Base Configuration Screen 136
19.3 The 802.1p Priority Table 138
19.4 The Tag Priority Table 139
19.5 The IP DSCP Priority Table 139
19.6 The Priority Override Configuration Screen 140

Part IV: Management 143

Chapter 20
Mgmt Config and System Restart Menu 145

20.1 Overview 145
20.2 The Serial Port Configuration Screen 145
20.3 The SNMP Configuration Screens 146
20.3.1 The SNMP Communities Screen 147
20.3.2 The IP Trap Manager Screen 147
20.4 The SNTP Screen 148
20.5 Alarms and Logs 150
20.6 The User Configuration Screen 151
20.7 The Cable Test Screen 152

20.8 The Host DoS Protection 153
20.9 The Port Abnormal Traffic Detection Screen 154
20.10 Upgrading the Firmware 155
20.11 Managing the Configuration File 156
20.12 Restarting the System 156

Part V: Troubleshooting & Product Specifications 159

Chapter 21
Troubleshooting 161

21.1 Power, Hardware Connections, and LEDs 161
21.2 Switch Access and Login 162

Chapter 22
Product Specifications 165

Part VI: Appendices and Index 169

Appendix A Changing a Fuse 171

Appendix B Common Services 173

Appendix C Legal Information 177

Index 181

PART I
Introduction and Hardware

Getting to Know Your Switch (19)

Hardware Installation and Connection (25)

Hardware Overview (29)

1

Getting to Know Your Switch

1.1 Introduction

This chapter introduces the main features and applications of the Switch.

The Switch is a layer-2 standalone Ethernet switch with additional layer-2, layer-3, and layer-4 features suitable for metro ethernets. The Switch has eight 10/100 Mbps Ethernet ports and two mini-GBIC slots. It also has two GbE dual personality interfaces with each interface comprising one mini-GBIC slot and one 10/100/1000 Mbps RJ-45 port, with either port or slot active at a time.

With its built-in web configurator, managing and configuring the Switch is easy. In addition, the Switch can also be managed via Telnet, any terminal emulator program on the console port, or third-party SNMP management.

See Chapter 22 on page 165 for a full list of software features available on the Switch.

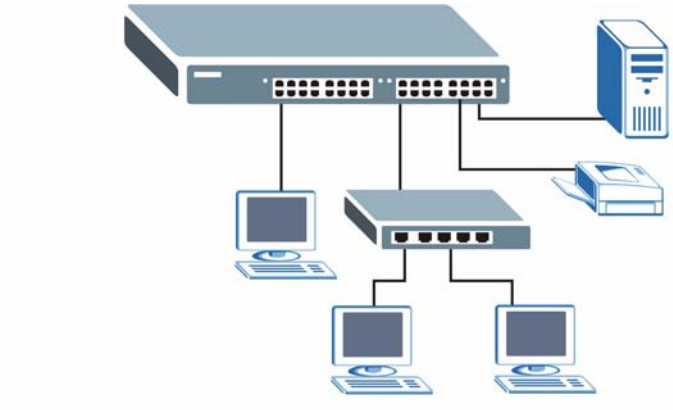
This section shows a few examples of using the Switch in various network environments.

1.1.1 Backbone Application

The Switch is an ideal solution for small networks where rapid growth can be expected in the near future. The Switch can be used standalone for a group of heavy traffic users. You can connect computers and servers directly to the Switch's port or connect other switches to the Switch.

In this example, all computers can share high-speed applications on the server. To expand the network, simply add more networking devices such as switches, routers, computers, print servers etc.

Figure 1 Backbone Application

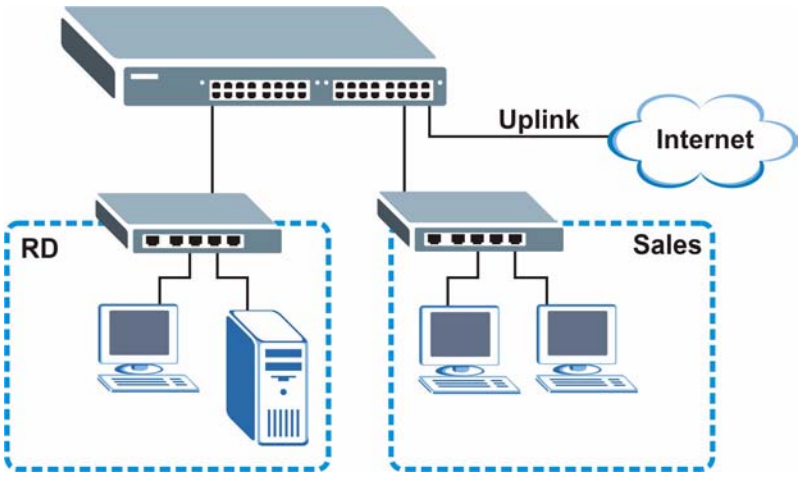


1.1.2 Bridging Example

In this example, the Switch connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the Switch. You can provide a super-fast uplink connection by using a Gigabit Ethernet/mini-GBIC port on the Switch.

Moreover, the Switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

Figure 2 Bridging Application

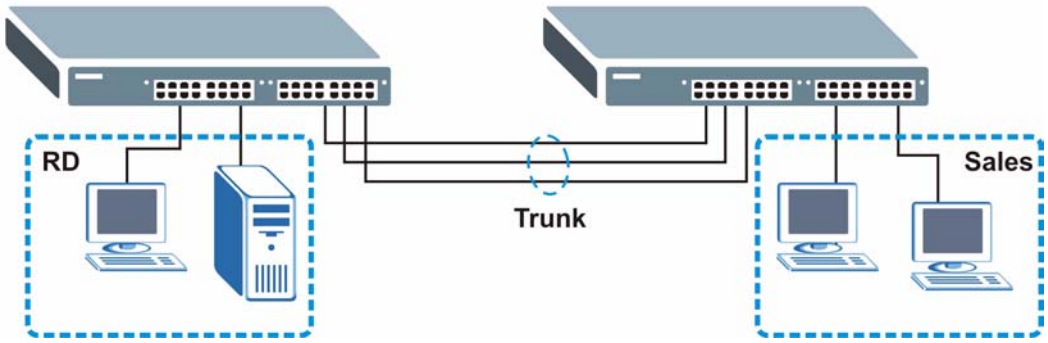


1.1.3 High Performance Switching Example

The Switch is ideal for connecting two networks that need high bandwidth. In the following example, use trunking to connect these two networks.

Switching to higher-speed LANs such as ATM (Asynchronous Transmission Mode) is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance. The Switch can provide the same bandwidth as ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

Figure 3 High Performance Switched Workgroup Application



1.1.4 IEEE 802.1Q VLAN Application Examples

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

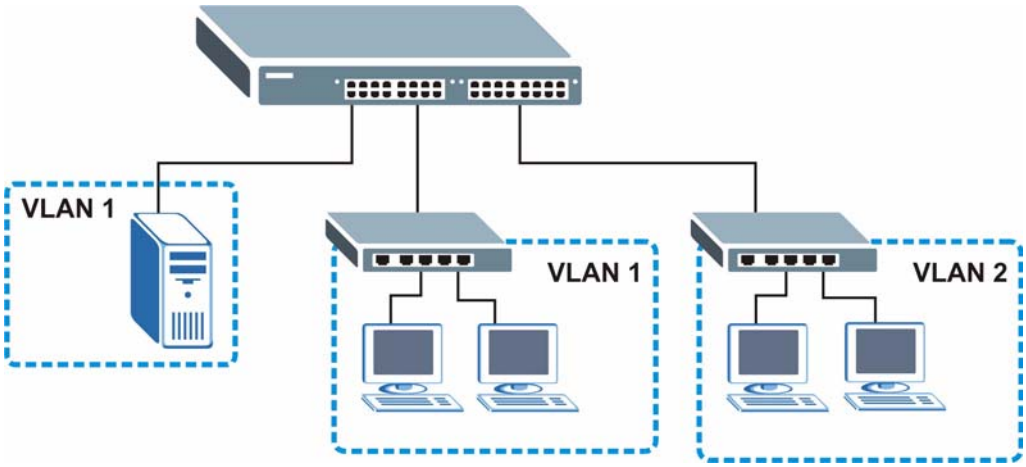
For more information on VLANs, refer to Chapter 11 on page 83.

1.1.4.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

Shared resources such as a server can be used by all ports in the same VLAN as the server. In the following figure only ports that need access to the server need to be part of VLAN 1. Ports can belong to other VLAN groups too.

Figure 4 Shared Server Using VLAN Example



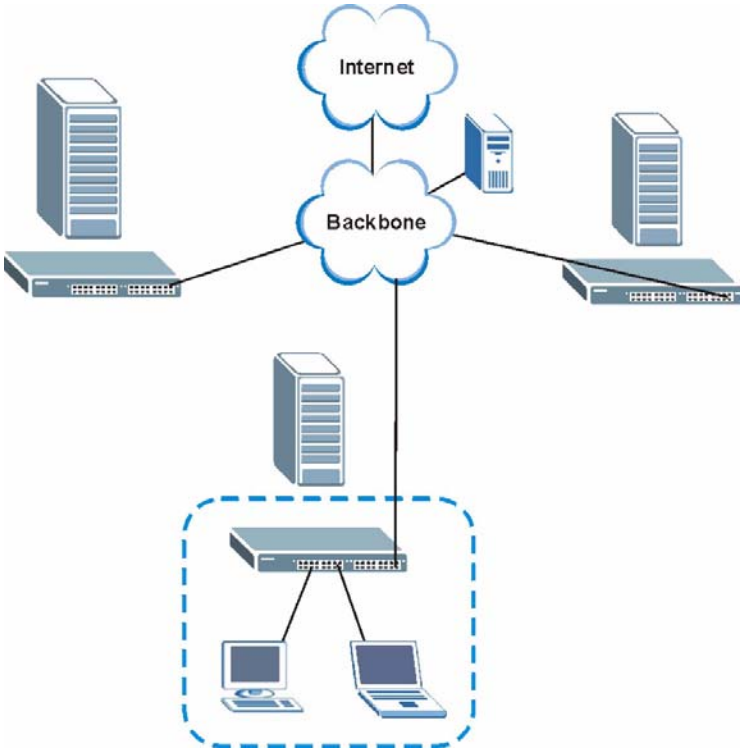
1.1.5 Metro Ethernet

The Switch is ideal for connecting users to an Ethernet network that spans a metropolitan area.

In the following example, the Switch is one of many switches that connect users in the metropolitan area to the Internet. The metro ethernet is based on a star (or hub-and-spoke) topology, though other topologies, such as ring or mesh, are also

possible. The Switch is connected to the backbone and the metropolitan servers over an optical network that provides higher bandwidth than copper.

Figure 5 Metro Ethernet



1.2 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See Chapter 4 on page 37.
- Command Line Interface. Line commands offer an alternative to the web configurator and in some cases are necessary to configure advanced features. See the CLI Reference Guide.
- SNMP. The Switch can be monitored by an SNMP manager. See Section 20.3 on page 146.

1.3 Good Habits for Managing the Switch

Do the following things regularly to make the Switch more secure and to manage the Switch more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the Switch to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Switch. You could simply restore your last configuration.

2

Hardware Installation and Connection

2.1 Installation Scenarios

This chapter shows you how to install and connect the Switch.

The Switch can be placed on a desktop or rack-mounted on a standard EIA rack. Use the rubber feet in a desktop installation and the brackets in a rack-mounted installation.

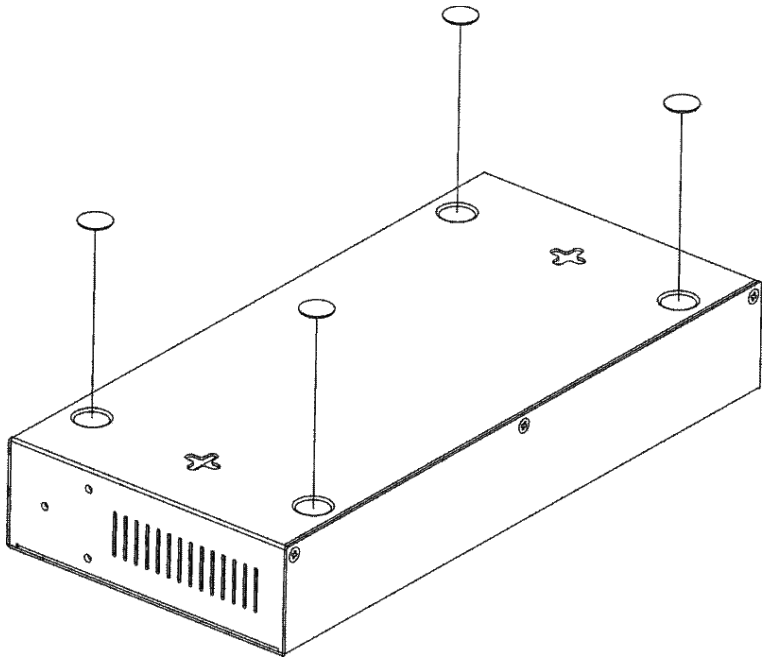
Note: For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the Switch. This is especially important for enclosed rack installations.

2.2 Desktop Installation Procedure

1. Make sure the Switch is clean and dry.
2. Set the Switch on a smooth, level surface strong enough to support the weight of the Switch and the connected cables. Make sure there is a power outlet nearby.
3. Make sure there is enough clearance around the Switch to allow air circulation and the attachment of cables and the power cord.
4. Remove the adhesive backing from the rubber feet.

5 Attach the rubber feet to each corner on the bottom of the Switch. These rubber feet help protect the Switch from shock or vibration and ensure space between devices when stacking.

Figure 6 Attaching Rubber Feet



Note: Do NOT block the ventilation holes. Leave space between devices when stacking.

2.3 Mounting the Switch on a Rack

The Switch can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your Switch on a standard EIA rack using a rack-mounting kit.

2.3.1 Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Philips screwdriver.
- Four M5 flat head screws and a #2 Philips screwdriver.

Failure to use the proper screws may damage the unit.

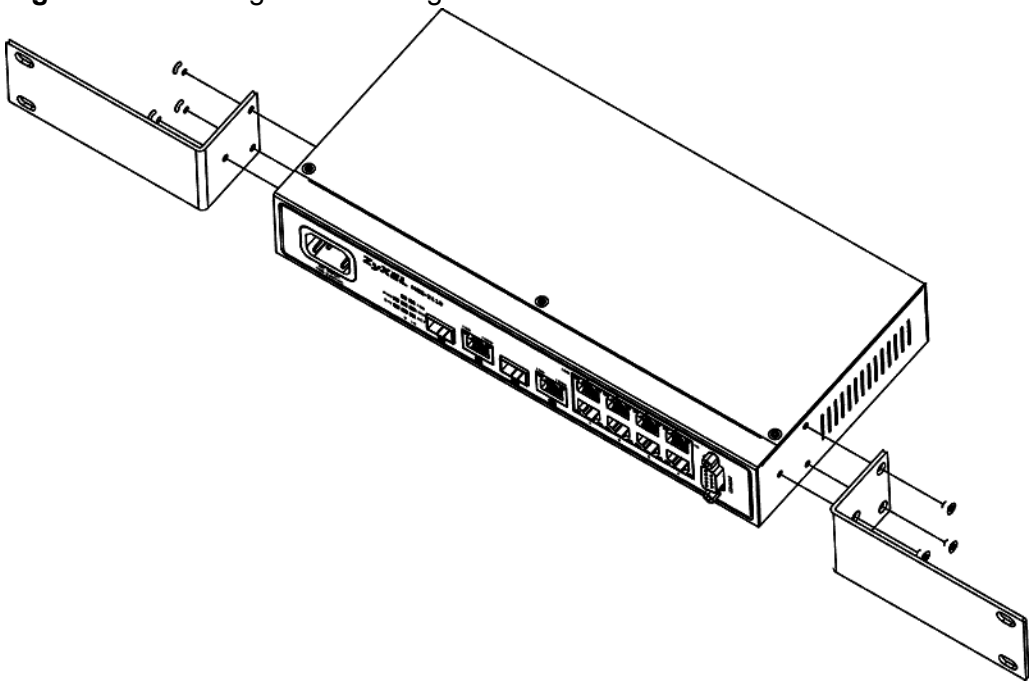
2.3.1.1 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains.
- Make sure the position of the Switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.3.2 Attaching the Mounting Brackets to the Switch

1 Position a mounting bracket on one side of the Switch, lining up the four screw holes on the bracket with the screw holes on the side of the Switch.

Figure 7 Attaching the Mounting Brackets



2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.

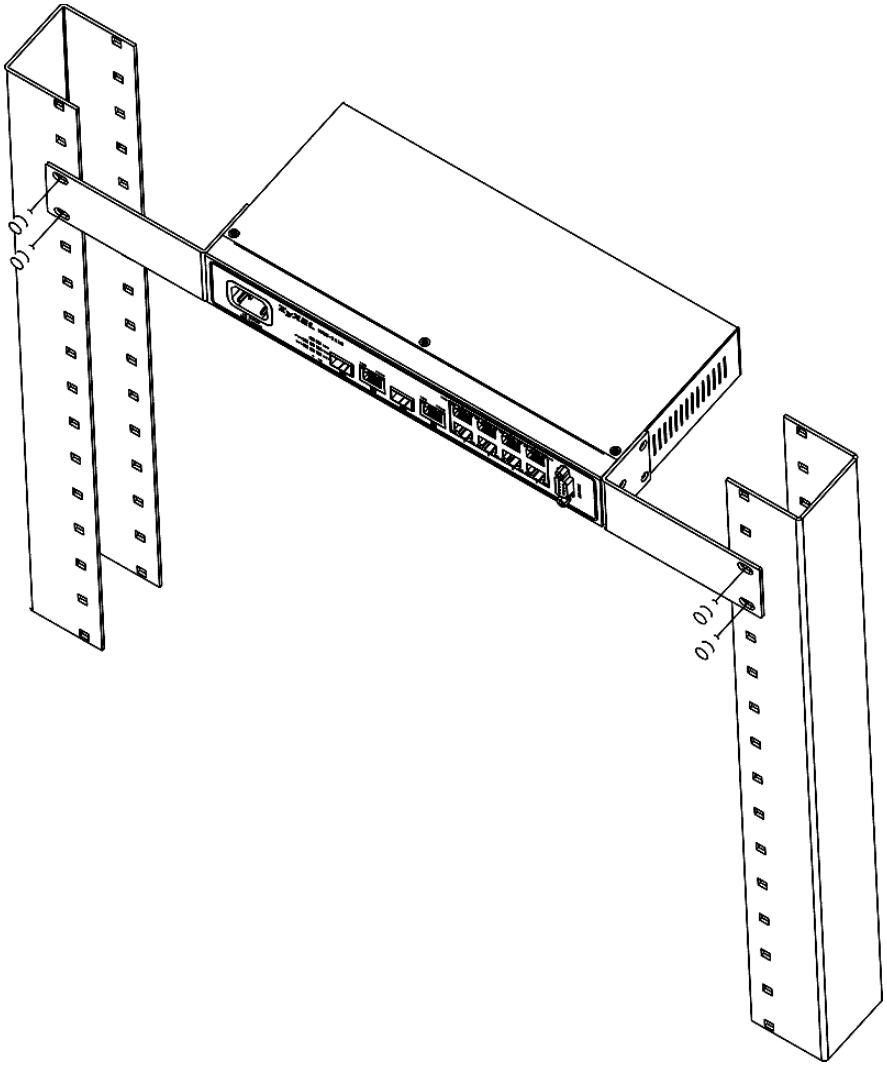
3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.

4 You may now mount the Switch on a rack. Proceed to the next section.

2.3.3 Mounting the Switch on a Rack

1 Position a mounting bracket (that is already attached to the Switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

Figure 8 Mounting the Switch on a Rack



2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.

3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

3

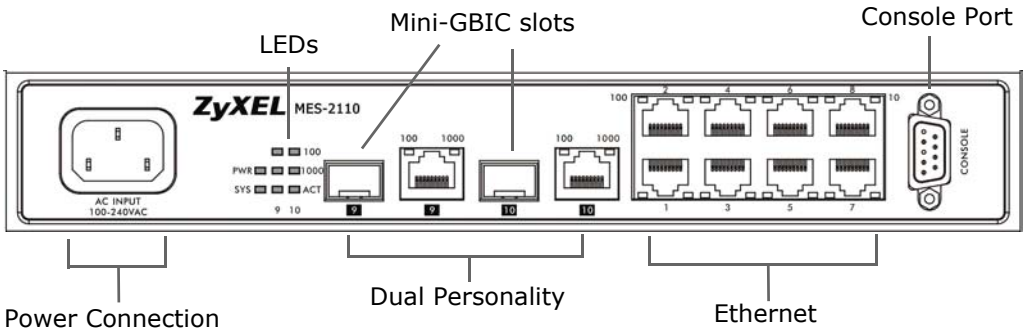
Hardware Overview

This chapter describes the front panel and rear panel of the Switch and shows you how to make the hardware connections.

3.1 Front Panel

The following figure shows the front panel of the Switch.

Figure 9 Front Panel I



The following table describes the port labels on the front panel.

Table 1 Front Panel Connections

LABEL	DESCRIPTION
Power Connection	Connect an appropriate power supply to this port.
8 10/100 Mbps RJ-45 Ethernet Ports	Connect these ports to a computer, a hub, an Ethernet switch or router.
Two Mini-GBIC Slots	Use mini-GBIC transceivers in these slots for fiber-optic or copper connections to backbone Ethernet switches.

Table 1 Front Panel Connections (continued)

LABEL	DESCRIPTION
Two Dual Personality Interfaces	Each interface has one 1000 Base-T copper RJ-45 port and one mini-GBIC slot, with one port active at a time.
	• 10/100/1000 Mbps RJ-45 GbE Ports: Connect these Gigabit Ethernet ports to high-bandwidth backbone network Ethernet switches.
	• Mini-GBIC Slots: Use mini-GBIC transceivers in these slots for fiber-optic or copper connections to backbone Ethernet switches.
Console Port	The console port is for local configuration of the Switch.

3.1.1 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100
- Terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port of the Switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.1.2 Gigabit Ethernet Ports

The Switch has 1000Base-T auto-negotiating, auto-crossover Ethernet ports. In 10/100/1000 Mbps Fast Ethernet, the speed can be 10 Mbps, 100 Mbps or 1000 Mbps and the duplex mode can be half duplex or full duplex.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (10/100/1000 Mbps) and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

Two of the 1000Base-T Ethernet ports are paired with a mini-GBIC slot to create a dual personality interface. The Switch uses up to one connection for each mini-GBIC and 1000Base-T Ethernet pair. The mini-GBIC slots have priority over the Gigabit ports. This means that if a mini-GBIC slot and the corresponding GbE port are connected at the same time, the GbE port will be disabled.

When auto-negotiation is turned on, a Ethernet port negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

3.1.2.1 Default Ethernet Negotiation Settings

The factory default negotiation settings for the Gigabit ports on the Switch are:

- Speed: Auto
- Duplex: Auto
- Flow control: Off
- Link Aggregation: Disabled

3.1.2.2 Auto-crossover

All ports are auto-crossover, that is auto-MDIX ports (Media Dependent Interface Crossover), so you may use either a straight-through Ethernet cable or crossover Ethernet cable for all Gigabit port connections. Auto-crossover ports automatically sense whether they need to function as crossover or straight ports, so crossover cables can connect both computers and switches/hubs.

3.1.3 Mini-GBIC Slots

These are slots for mini-GBIC (Gigabit Interface Converter) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. The Switch does not come with transceivers. You must use transceivers that comply with the Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

You can change transceivers while the Switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic or even copper cable connectors.

To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

- Type: SFP connection interface
- Connection speed: 1 Gigabit per second (Gbps)

3.1.3.1 Transceiver Installation

Use the following steps to install a mini-GBIC transceiver (SFP module).

1. Insert the transceiver into the slot with the exposed section of PCB board facing down.
2. Press the transceiver firmly until it clicks into place.
3. The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.
4. Close the transceiver's latch (latch styles vary).
5. Connect the fiber optic cables to the transceiver.

Figure 10 Transceiver Installation Example

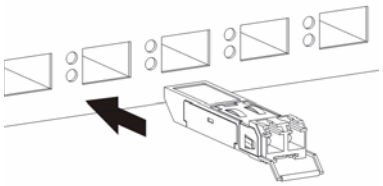
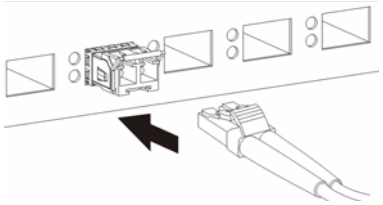


Figure 11 Connecting the Fiber Optic Cables



3.1.3.2 Transceiver Removal

Use the following steps to remove a mini-GBIC transceiver (SFP module).

1. Remove the fiber optic cables from the transceiver.
2. Open the transceiver's latch (latch styles vary).

3 Pull the transceiver out of the slot.

Figure 12 Removing the Fiber Optic Cables

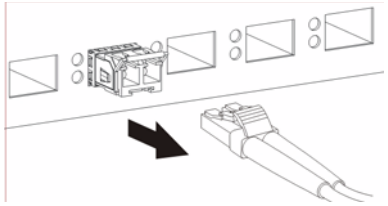


Figure 13 Opening the Transceiver's Latch Example

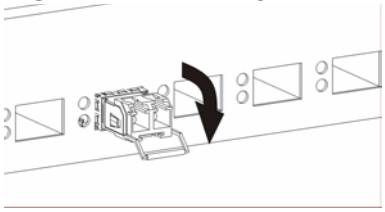
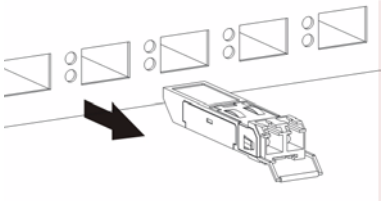


Figure 14 Transceiver Removal Example



3.1.4 Power Connector

Note: Make sure you are using the correct power source as shown on the panel.

To connect power to the Switch, insert the female end of the power cord the power receptacle on the front panel. Connect the other end of the supplied power cord to a power outlet. Make sure that no objects obstruct the airflow of the fans (located on the side of the unit).

The Switch requires a power supply of 100-240 VAC, 50/60 Hz, 0.55 A Max.

See Chapter 22 on page 165 for information on the Switch's power supply requirements.

3.2 LEDs

After you connect the power to the Switch, view the LEDs to ensure proper functioning of the Switch and as an aid in troubleshooting.

Table 2 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The system is turned on.
		Off	The system is off.
SYS	Green	On	The system is on and functioning properly.
		Blinking	The system is rebooting and performing self-diagnostic tests.
		Off	The power is off or the system is not ready/malfunctioning.
Ethernet Ports			
LINK/ ACT	Green	Blinking	The system is transmitting/receiving to/from a 10 Mbps Ethernet network.
		On	The link to a 10 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
Mini-GBIC Slots			
LNK	Green	On	The link to this port is up.
		Off	The link to this port is not connected.
ACT	Green	On	The link to an Ethernet network is on.
		Blinking	This port is receiving or transmitting data.
		Off	The port is not receiving or transmitting data.
1000Base-T Ethernet Ports (in Dual Personality Interface)			
ACT	Green	Blinking	The system is transmitting/receiving to/from a 10 Mbps or a 1000 Mbps Ethernet network.
		On	The link to a 10 Mbps or a 1000 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.

PART II
Basic Configuration

The Web Configurator (37)

System Details (47)

4

The Web Configurator

4.1 Introduction

This section introduces the configuration and functions of the web configurator.

The web configurator is an HTML-based management interface that allows easy Switch setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

4.2 System Login

1. Start your web browser.
2. Type "http://" and the IP address of the Switch (for example, the default is 192.168.1.1) in the Location or Address field. Press [ENTER].

3 The login screen appears. Enter the user name (**admin** by default) and password (**1234** by default).

Figure 15 Web Configurator: Login

Connect to 192.168.1.1
The server 192.168.1.1 at Web Manager requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

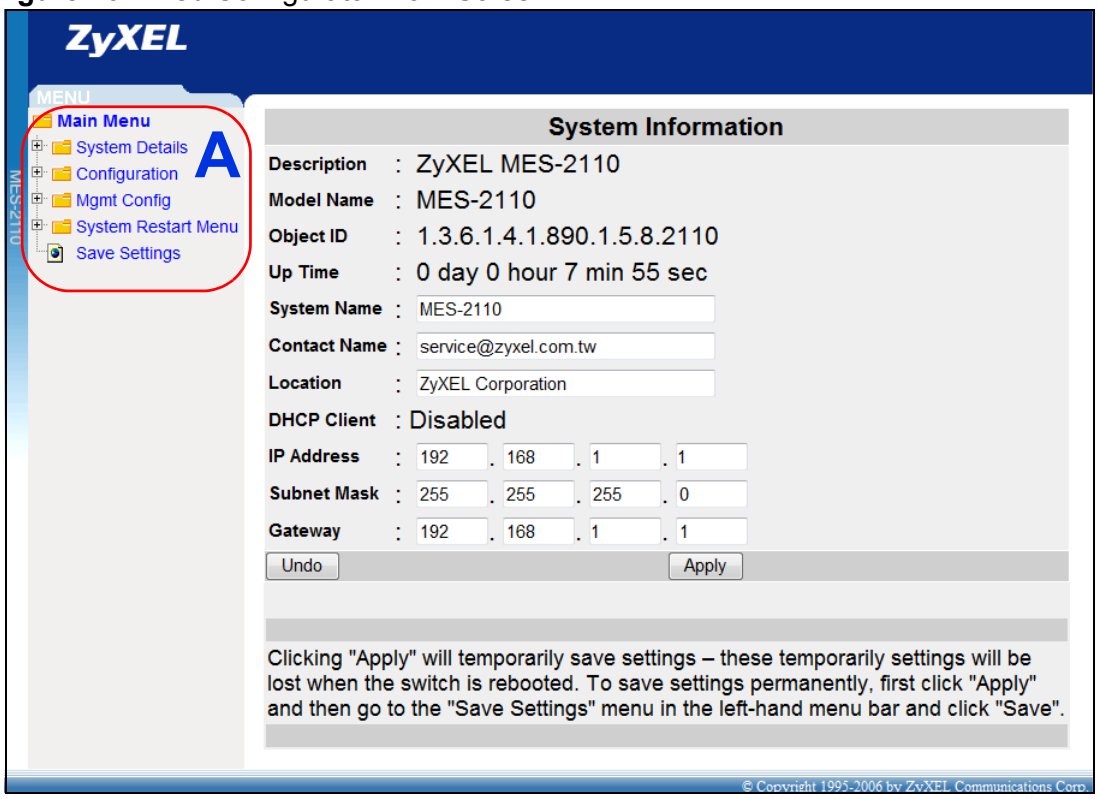
4 Click **OK** to view the first web configurator screen.

4.3 The Main Screen

The **Main** screen is the first screen that displays when you access the web configurator.

The following figure shows the navigating components of a web configurator screen.

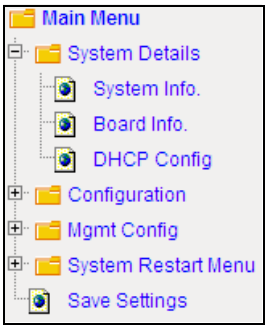
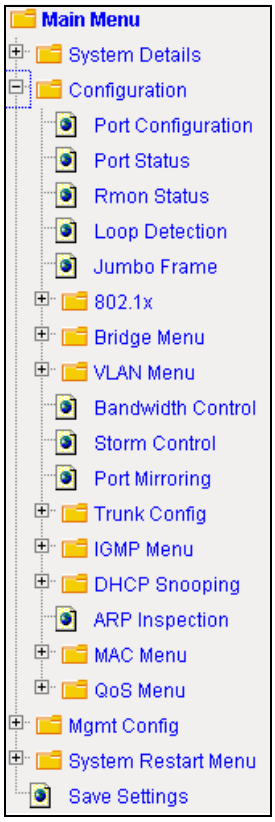
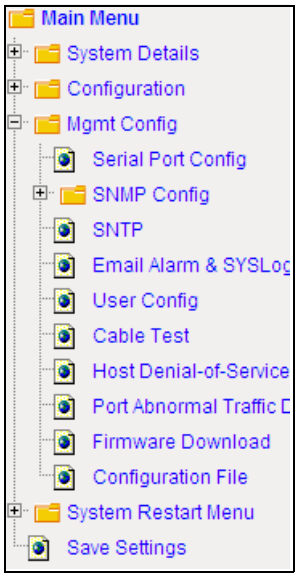
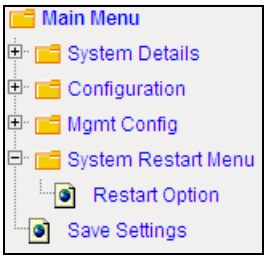
Figure 16 Web Configurator Main Screen


ZyXEL
MENU
Main Menu
System Details
Configuration
Mgmt Config
System Restart Menu
Save Settings
A
MES-2110
System Information
Description : ZyXEL MES-2110
Model Name : MES-2110
Object ID : 1.3.6.1.4.1.890.1.5.8.2110
Up Time : 0 day 0 hour 7 min 55 sec
System Name : MES-2110
Contact Name : service@zyxel.com.tw
Location : ZyXEL Corporation
DHCP Client : Disabled
IP Address : 192 . 168 . 1 . 1
Subnet Mask : 255 . 255 . 255 . 0
Gateway : 192 . 168 . 1 . 1
Undo
Apply
Clicking "Apply" will temporarily save settings – these temporarily settings will be lost when the switch is rebooted. To save settings permanently, first click "Apply" and then go to the "Save Settings" menu in the left-hand menu bar and click "Save".
© Copyright 1995-2006 by ZyXEL Communications Corp.

A - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window.

In the navigation panel, click a main link to reveal a list of submenu links.

Table 3 Navigation Panel Sub-links Overview

SYSTEM DETAILS	CONFIGURATION	MGMT CONFIG	SYSTEM RESTART MENU
			

The following table lists the various web configurator screens within the sub-links.

Table 4 Web Configurator Screen Sub-links Details

SYSTEM DETAILS	CONFIGURATION	MGMT CONFIG	SYSTEM RESTART MENU
System Info. Board Info. DHCP Config	Port Configuration Port Status Rmon Status Loop Detection Jumbo Frame 802.1 Global Configuration RADIUS Server Configuration Port Configuration 802.1x Status Bridge Menu Bridge Config RSTP System Config RSTP Per Port Config VLAN Menu VLAN Type Port-Based Tag-Based (802.1q) VLAN Stacking Port Info. Tag-Based Info. Management VLAN Bandwidth Control Storm Control Port Mirroring Trunk Config Aggregator Setting LACP Configuration LACP Link Status IGMP Menu IGMP Config IGMP Groups Status MVR	Serial Port Config SNMP Config SNMP Communities IP Trap Manager SNTP Email Alarm & SYSLog User Config Cable Test Host Denial-of-Service Protection Port Abnormal Traffic Detection Firmware Download Configuration File	Restart Option

	DHCP Snooping DHCP Snooping Config DHCP Binding Table ARP Inspection MAC Menu MAC Table Status Lock Learning MAC MAC Filter Config MAC Limit Config QoS Menu Base Configuration 802.1p Priority Tag Priority IP DSCP Priority Priority Override Configuration		

The following table describes the links in the navigation panel.

Table 5 Navigation Panel Links

LINK	DESCRIPTION
System Details	
System Info.	This link takes you to a screen that displays general system information. You can also configure general system information about the Switch.
Board Info.	This link takes you to a screen that shows hardware and firmware information.
DHCP Config	This link takes you to a screen where you can configure the DHCP settings.
Configuration	
Port Configuration	This link takes you to a screen where you can configure settings for individual Switch ports.
Port Status	This link takes you to a screen that shows port settings for individual Switch ports.
Rmon Status	This link takes you to a screen where you can view statistics on the traffic going through each port.
Loop Detection	This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network.
Jumbo Frame	This link takes you to a screen where you can configure Jumbo frames or Ethernet frames with a payload greater than 1500 bytes.Use this screen to configure the jumbo frame size.
802.1x	This link takes you to a screen where you can configure IEEE 802.1x authentication.
Bridge Menu	This link takes you to screens where you can configure the RSTP to prevent network loops.
VLAN Menu	This link takes you to screens where you can configure port-based or tag-based (802.1Q) VLAN (depending on what you configured in the Switch Setup menu).

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
Bandwidth Control	This link takes you to a screen where you can configure bandwidth limits on the Switch.
Storm Control	This link takes you to a screen to set up broadcast filters.
Port Mirroring	This link takes you to a screen where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Trunk Config	This link takes you to screens where you can logically aggregate physical links to form one logical, higher-bandwidth link.
IGMP Menu	This link takes you to screens where you can configure various multicast features, IGMP snooping and create multicast VLANs.
DHCP Snooping	This link takes you to screens where you can configure filtering of unauthorized DHCP frames in your network.
ARP Inspection	This link takes you to a screen where you can configure filtering of unauthorized Address Resolution Protocol (ARP) frames in your network.
MAC Menu	This link takes you to screens where you can configure the following settings: • configure IEEE 802.1x port authentication as well as MAC authentication for clients communicating via the Switch, • activate MAC address learning and set the maximum number of MAC addresses to learn on a port, • view the MAC addresses (and types) of devices attached to what ports.
QoS Menu	This link takes you to screens where you can configure priority levels for traffic transmitted through each port.
Mgmt Config	
Serial Port Config	This link takes you to a screen where you can configure the parameters for connections via the console port.
SNMP Config	This link takes you to screens where you can configure settings for date and time.
SNTP	This link takes you to a screen where you can configure SNTP and date/time settings.
Email Alarm & SYSLog	This link takes you to screens where you can set up system logs and e-mail the logs to you.
User Config	This link takes you to a screen where you can set up administrative and user accounts for people to use the Switch.
Cable Test	This link takes you to a screen where you can test the cable connection on each port.
Host Denial-of-Service Protection	This link takes you to a screen where you can allow trusted computers to access the Switch via remote management.
Port Abnormal Traffic Detection	This link takes you to a screen where you can configure the Switch to detect abnormal traffic transmission and temporarily or permanently block traffic transmission through a port.

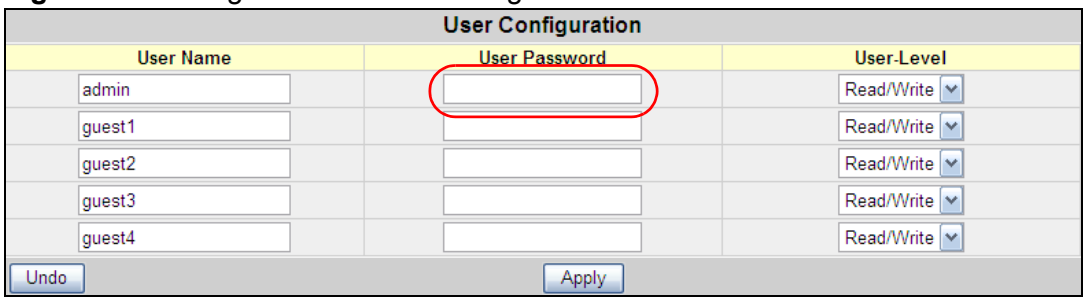
Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
Firmware Download	This link takes you to a screen where you can perform firmware maintenance.
Configuration File	This link takes you to a screen where you can perform configuration file maintenance.
System Restart Menu	
Restart Option	This link takes you to a screen where you can reboot the system.
Save Settings	This link takes you to a screen where you can save the changes you have made on the Switch and restart the Switch.

4.3.1 Set Up the Administrative Password

After you log in for the first time, it is recommended you set up an administrator password. Click **Mgmt Config** > **User Config** to display the next screen. Enter a password for the **admin** account and click **Apply**.

Figure 17 Configure Administrator Login Password



4.4 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Click the **Save Settings** link in the navigation panel to save your configuration to nonvolatile memory. Nonvolatile memory refers to the Switch's storage that remains even if the Switch's power is turned off. If you don't use **Save Settings** all configuration changes will only apply until you restart the Switch.

Note: Use the **Save Settings** link when you are done with a configuration session.

4.5 Switch Lockout

You could block yourself (and all others) from using in-band-management (managing through the data ports) if you do one of the following:

1. Delete the management VLAN (default is VLAN 1).
2. Delete all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the Switch.
3. Filter all traffic to the CPU port.
4. Disable all ports.
5. Misconfigure the text configuration file.
6. Forget the password and/or IP address.
7. Prevent all services from accessing the Switch.
8. Change a service port number but forget it.

Note: Be careful not to lock yourself and others out of the Switch. If you do lock yourself out, try using out-of-band management (via the console port) to configure the Switch.

4.6 Resetting the Switch

If you lock yourself (and others) from the Switch or forget the administrator password, you will need to reload the factory-default configuration file or reset the Switch back to the factory defaults.

4.6.1 Reload the Configuration File

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600 bps with 8 data bits, no parity, one stop bit and flow control set to none. The password will also be cleared and the IP address be set to 192.168.0.254.

To upload the configuration file, do the following:

1. Connect to the console port using a computer with terminal emulation software.

2 Disconnect and reconnect the Switch's power to begin a session. When you reconnect the Switch's power, you will see the initial screen.

3 When you see "`Username:`", type `admin` and press [Enter].

4 Type the administrative password and press [Enter]. Simply press [Enter] if you did not set up a password.

5 Type `enable` and press [Enter] to turn on administrative commands.

6 Type `reset default` and press [Enter] to restore the system to the factory defaults. The Switch will restart.

Figure 18 Resetting the Switch: Via the Console Port

```
Username: admin
Password:
MES-2110> enable

MES-2110# reset default
```

The Switch is now reinitialized with a default configuration file.

5

System Details

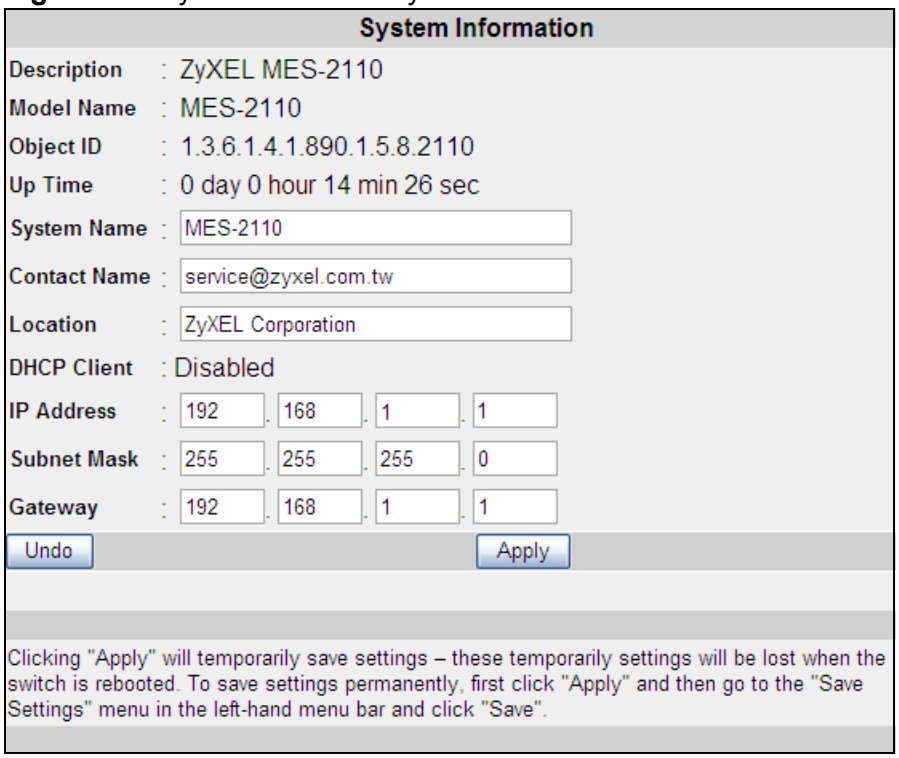
5.1 Overview

The **System Details** screens show general system information about the Switch. You can also use the screens to configure system and DHCP client settings.

5.2 The System Information Screen

Click **System Details** > **System Info.** to open the following screen.

Figure 19 System Details > System Info.


System Information
Description : ZyXEL MES-2110
Model Name : MES-2110
Object ID : 1.3.6.1.4.1.890.1.5.8.2110
Up Time : 0 day 0 hour 14 min 26 sec
System Name : MES-2110
Contact Name : service@zyxel.com.tw
Location : ZyXEL Corporation
DHCP Client : Disabled
IP Address : 192 . 168 . 1 . 1
Subnet Mask : 255 . 255 . 255 . 0
Gateway : 192 . 168 . 1 . 1
Undo
Apply
Clicking "Apply" will temporarily save settings – these temporarily settings will be lost when the switch is rebooted. To save settings permanently, first click "Apply" and then go to the "Save Settings" menu in the left-hand menu bar and click "Save".

The following table describes the labels in this screen.

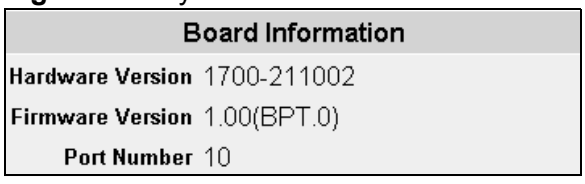
Table 6 System Details > System Info.

LABEL	DESCRIPTION
Description	This is the descriptive name of the Switch for identification purposes.
Model Name	This is the model name of the Switch.
Object ID	An Object ID defines what trap the Switch should send an SNMP Manager.
Up Time	This shows how long the Switch has been turned on.
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Contact Name	Enter the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Location	Enter the geographic location of your Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
DHCP Client	This shows whether the DHCP client is **Enabled** or **Disabled**. If DHCP is disabled, you must enter an IP address, subnet mask and gateway in the following fields. Otherwise, a DHCP server will assign this information to the Switch. See Section 5.4 on page 49 for details about configuring the DHCP client.
IP Address	Enter the IP address of your Switch in dotted decimal notation for example 192.168.1.1.
Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

5.3 The Board Information Screen

Use this screen to view the hardware and firmware information. Click **System Details** > **Board Info.** to open the following screen.

Figure 20 System Details > Board Info.



The following table describes the labels in this screen.

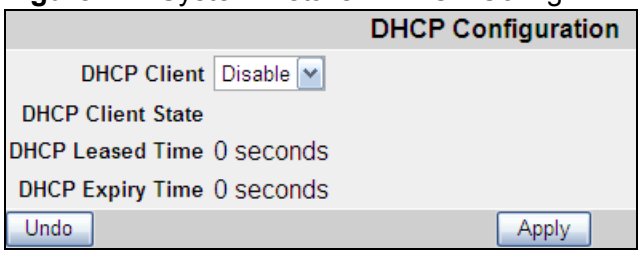
Table 7 System Details > Board Info.

LABEL	DESCRIPTION
Hardware Version	This is the version number of the Switch's hardware.
Firmware Version	This is the version number of the Switch's current firmware including the date and time that the firmware is created.
Port Number	This shows the number of available ports on the Switch.

5.4 The DHCP Configuration Screen

Use this screen to turn on or off the DHCP client. Click **System Details** > **DHCP Config** to open the following screen.

Figure 21 System Details > DHCP Config



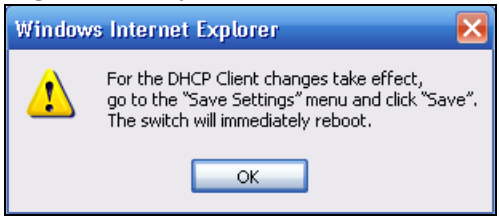
The following table describes the labels in this screen.

Table 8 System Details > DHCP Config

LABEL	DESCRIPTION
DHCP Client	Use this to turn the DHCP client on or off. Turn on the DHCP client if you have a DHCP server that can assign the Switch an IP address, subnet mask and a default gateway IP address automatically.
DHCP Client State	This shows whether the DHCP client is **Enabled** or **Disabled**.
DHCP Leased Time	This is how long ago the Switch got an IP address from a DHCP server (if DHCP client is enabled).
DHCP Expiry Time	This is how long there is to go before the Switch will get a new IP address from a DHCP server (if DHCP client is enabled).
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

Once you click the **Apply** button, the following message displays, reminding you to save your settings in the **Save Settings** screen and reboot the Switch.

Figure 22 System Details > DHCP Config > Apply


Windows Internet Explorer
For the DHCP Client changes take effect,
go to the "Save Settings" menu and click "Save".
The switch will immediately reboot.
OK

PART III
Configuration

Configuration (53)

Loop Detection (59)

Bridge (75)

VLAN (83)

Bandwidth Control (95)

Broadcast Storm Control (97)

Port Mirroring (99)

Link Aggregation (101)

IGMP (107)

IP Source Guard (119)

MAC (127)

QoS (135)

6

Configuration

6.1 Overview

The **Configuration** screens let you configure the Switch settings.

6.2 The Port Configuration Screen

Use this screen to configure Switch port settings. You can assign a unique name to the ports, select its speed setting and enable or disable auto-negotiation. Click **Configuration** > **Port Configuration** to open the following screen.

Figure 23 Configuration > Port Configuration

Port Configuration

Port	Name	Type	Admin	Speed		Duplex		Link	AUTO	Flow-Control
				Status	Setting	Status	Setting			
Port1		RJ45	Enable	100M	100M	Full	Full	Up	Enable	Enable
Port2		RJ45	Enable	100M	100M	Full	Full	Down	Enable	Enable
Port3		RJ45	Enable	100M	100M	Full	Full	Down	Enable	Enable
Port4		RJ45	Enable	100M	100M	Full	Full	Down	Enable	Enable
Port5		RJ45	Enable	100M	100M	Full	Full	Down	Enable	Enable
Port6		RJ45	Enable	100M	100M	Full	Full	Down	Enable	Enable
Port7		RJ45	Enable	100M	100M	Full	Full	Down	Enable	Enable
Port8		RJ45	Enable	100M	100M	Full	Full	Down	Enable	Enable
Port9		Fiber	Enable	1000M	N/A	Full	N/A	Down	N/A	Enable
Port10		Fiber	Enable	1000M	N/A	Full	N/A	Down	N/A	Enable

Undo Apply

The following table describes the labels in this screen.

Table 9 Configuration > Port Configuration

LABEL	DESCRIPTION
Port	This is the port number.
Name	Enter a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitation, the port name may be truncated in some web configurator screens.
Type	This is the type of connector for each port. Port 1-8 are RJ-45 ports for Ethernet connections. Port 9-10 are Gigabit SFP ports for fiber connections.
Admin	Use this to enable or disable administrative access.
Speed	The **Status** field shows the port's current speed (**10M** for 10 Mbps and **100M** for 100 Mbps). The **Setting** field is configurable when you disable the auto-negotiation function in the **AUTO** field. Use this field to set the port speed to either **10M** or **100M**. The speed for the fiber ports is fixed.
Duplex	The **Status** column shows the the port's duplex status. The **Setting** field is configurable when you disable the auto-negotiation function in the **AUTO** field. Use this field to change the status to **Half** or **Full** duplex mode. The duplex status for the fiber ports is fixed.
Link	This shows the port's connection status.
AUTO	Use this to enable or disable auto-negotiation. **AUTO** (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.

Table 9 Configuration > Port Configuration

LABEL	DESCRIPTION
Flow-Control	Use this to enable or disable flow control. A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing frame discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of frame collision) causing the sending port to temporarily stop sending signals and resend later. Select **Flow Control** to enable it.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

6.3 The Port Status Screen

To view the port statistics, click **Configuration** > **Port Status** to display the **Status** screen as shown next.

Figure 24 Configuration > Port Status

Ports Status

Port	Name	Type	Admin	Speed	Duplex	Link	AUTO	Flow-Control
Port1		RJ45	Enabled	100M	Full	Up	On	Enabled
Port2		RJ45	Enabled	100M	Full	Down	On	Enabled
Port3		RJ45	Enabled	100M	Full	Down	On	Enabled
Port4		RJ45	Enabled	100M	Full	Down	On	Enabled
Port5		RJ45	Enabled	100M	Full	Down	On	Enabled
Port6		RJ45	Enabled	100M	Full	Down	On	Enabled
Port7		RJ45	Enabled	100M	Full	Down	On	Enabled
Port8		RJ45	Enabled	100M	Full	Down	On	Enabled
Port9		Fiber	Enabled	1000M	Full	Down	On	Enabled
Port10		Fiber	Enabled	1000M	Full	Down	On	Enabled

Port Configuration

The following table describes the labels in this screen.

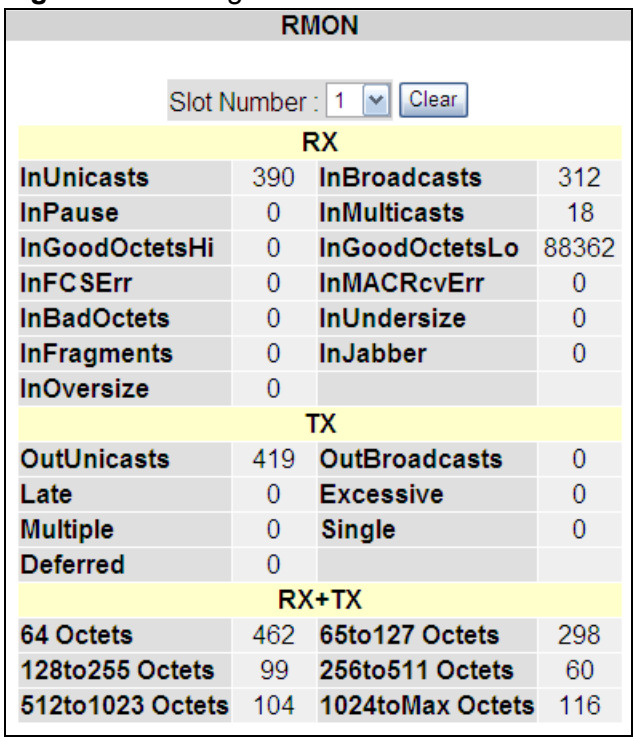
Table 10 Configuration > Port Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port.
Name	This is the name you assigned to this port in the **Configuration** > **Port Configuration** screen.
Type	This is the type of connector for each port. Port 1-8 are RJ-45 ports for Ethernet connections. Port 9-10 are Gigabit SFP ports for fiber connections.
Admin	This shows whether administrative access is **Enabled** or **Disabled** on the port. When administrative access is disabled on the port, users cannot manage the Switch via that port.
Speed	This is the port's current speed (**10M** for 10 Mbps and **100M** for 100 Mbps).
Duplex	This is the the port's duplex status (**Half** or **Full**).
Link	This shows the port's connection status.
AUTO	This shows whether auto-negotiation is **On** or **Off**.
Flow-Control	This shows whether flow control is **Enabled** or **Disabled**.
Port Configuration	Click this to configure port settings in the **Port Configuration** screen.

6.4 The RMON Status Screen

Use this screen to view individual port statistics. Click **Configuration** > **Rmon Status** to open the following screen.

Figure 25 Configuration > Rmon Status



The following table describes the labels in this screen.

Table 11 Configuration > Rmon Status

LABEL	DESCRIPTION
Slot Number	Use this to select the port number you are viewing.
Clear	Click this to reset the statistics on this port to zero.
RX The following fields show detailed information about frames received.	
InUnicasts	This field shows the number of good unicast frames received.
InBroadcasts	This field shows the number of good broadcast frames received.
InPause	This field shows the number of 802.3x Pause frames received.
InMulticasts	This field shows the number of good multicast frames received.
InGoodOctetsHi	This field shows the number of good upper octet frames received.
InGoodOctetsLo	This field shows the number of good lower octet frames received.
InFCSErr	This field shows the number of frames received with Cyclic Redundant Check (CRC) error(s).
InMACRcvErr	This field shows the number of frames received with an RxErr signal from the PHY.

Table 11 Configuration > Rmon Status (continued)

LABEL	DESCRIPTION
InBadOctets	This field shows the number of bad octet frames received.
InUndersize	This field shows the number of frames received that were too short (shorter than 64 octets).
InFragments	This field shows the number of frames received that were too short (shorter than 64 octets) and were received with with Cyclical Redundancy Check (CRC) errors.
InJabber	This field shows the number of frames received with a length that exceeds the maximum octet size and were received with CRC errors.
InOversize	This field shows the number of frames received with a length that was out of range.
TX The following fields show detailed information about frames transmitted.	
OutUnicasts	This field shows the number of good unicast frames transmitted.
OutBroadcasts	This field shows the number of good broadcast frames transmitted.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the frames have already been transmitted.
Excessive	This is a count of frames for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Multiple	This is a count of successfully transmitted frames for which transmission was inhibited by more than one collision.
Single	This is a count of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Deferred	This is a count of frames for which transmission delayed due to busy traffic. The deferred frames are waiting to be transmitted from the Switch buffer. This counter only works for the half-duplex mode.
RX+TX	
64 Octets	This field shows the number of frames (including bad frames) received that were 64 octets in length.
65to127 Octets	This field shows the number of frames (including bad frames) received that were between 65 and 127 octets in length.
128to255 Octets	This field shows the number of frames (including bad frames) received that were between 128 and 255 octets in length.
256to511 Octets	This field shows the number of frames (including bad frames) received that were between 256 and 511 octets in length.
512to1023 Octets	This field shows the number of frames (including bad frames) received that were between 512 and 1023 octets in length.
1024toMax Octets	This field shows the number of frames (including bad frames) received that were between 1024 and the maximum octets in length.

7

Loop Detection

7.1 Overview

Loop detection allows you to configure the Switch to shut down a port if it detects that frames sent out on that port loop back to the Switch.

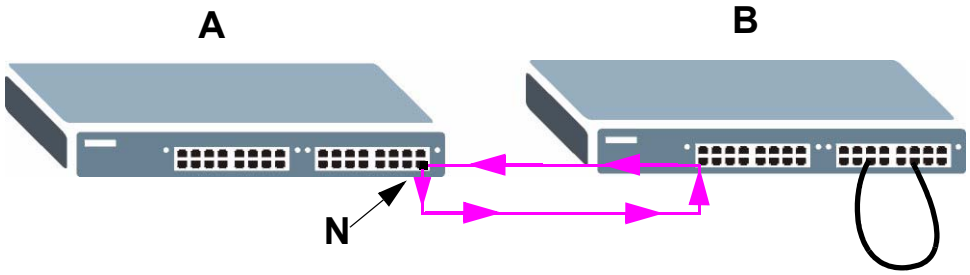
Loop detection is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast frames leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from B.

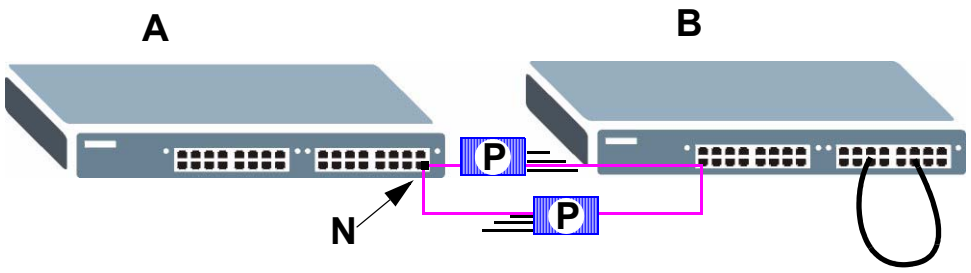
Figure 26 Switch in Loop State



The loop detection feature checks to see if a loop detection enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe frame and seeing if the frame returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

The following figure shows a loop detection enabled port **N** on switch **A** sending a probe frame **P** to switch **B**. Since switch **B** is in loop state, the probe frame **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

Figure 27 Loop detection - Probe Frame

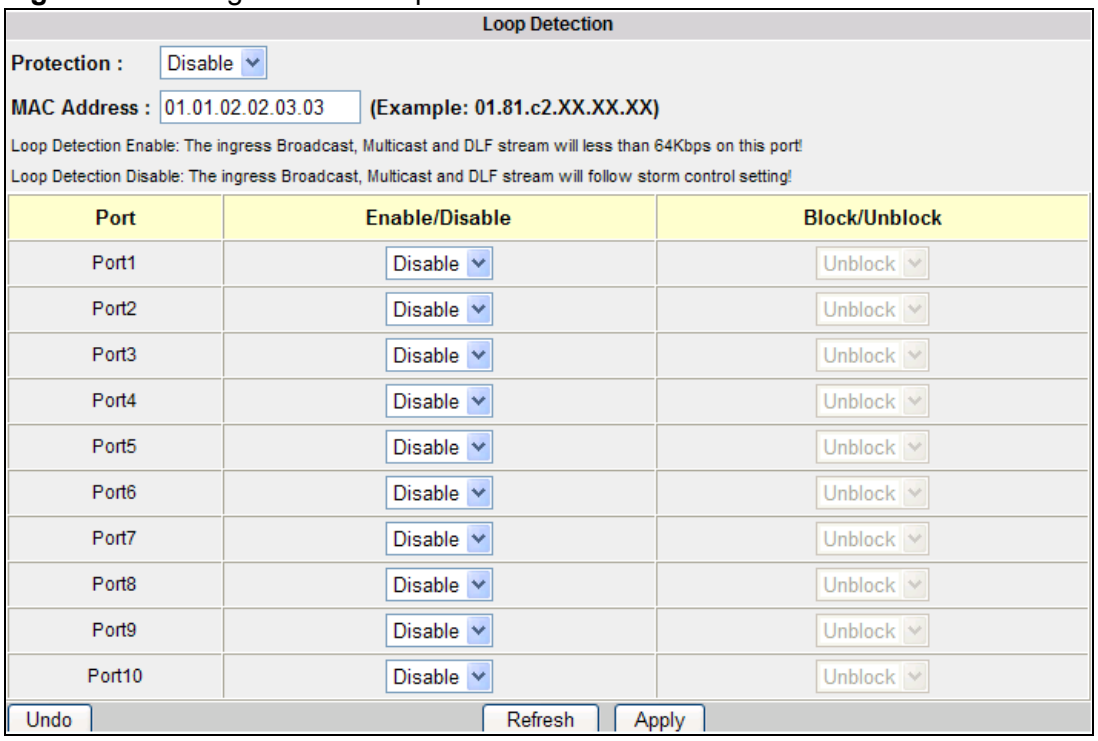


Note: After resolving the loop problem on your network you can re-activate the disabled port via the web configurator or via commands (See the CLI Reference Guide).

7.2 The Loop Detection Screen

Click **Configuration** > **Loop Detection** to open the following screen.

Figure 28 Configuration > Loop Detection



The following table describes the labels in this screen.

Table 12 Configuration > Loop Detection

LABEL	DESCRIPTION
Protection	Select **Enable** or **Disable** to have the Switch apply loop detection. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop detection feature.
MAC Address	This is the MAC address of the probe frame sent by the Switch. You can configure the field as a unicast or multicast MAC address, depending on your needs. The default MAC address is a multicast address (01.01.02.02.03.03). Some network switch does not forward frames with unrecognized multicast MAC address. Test frames sent out for loop detection will be discarded by this type of switch. Users can configure a unicast MAC address to solve this problem.
Port	This is the port number.
Enable/Disable	Select **Enable** or **Disable** to have the Switch apply loop detection feature on this port. When the loop detection feature is enabled, the Switch sends probe frames from this port to check if the switch it is connected to is in loop state. If the switch that this port is connected is in loop state the Switch will shut down this port.
Block/Unblock	When the Switch detects looping, the system sets the port to **Block**. Use this field to **Unblock** the port once you have manually fixed the loop.
Undo	Click this to restore your last saved settings.
Refresh	Click this to reset the data for the field(s).
Apply	Click this to save your changes.

8

Jumbo Frame

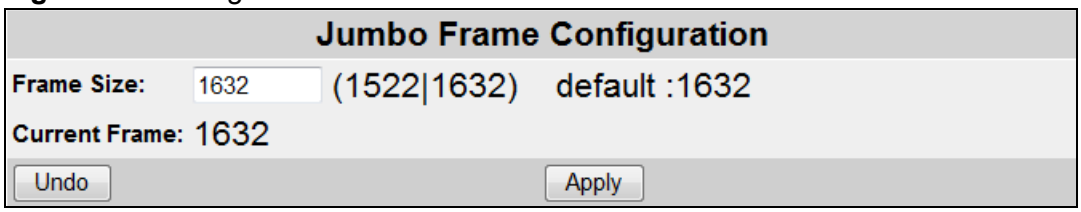
8.1 Overview

Jumbo frames are Ethernet frames with a payload greater than 1500 bytes. Jumbo frames can enhance data transmission efficiency in a Gigabit network.

8.2 The Jumbo Frame Configuration Screen

Use this screen to configure the jumbo frame size. Click **Configuration** > **Jumbo Frame** to open the following screen.

Figure 29 Configuration > Jumbo Frame



The following table describes the labels in this screen.

Table 13 Configuration > Jumbo Frame

LABEL	DESCRIPTION
Frame Size	Configure the jumbo frame size (1522 to 1632). The bigger the frame size, the better the performance.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

9

802.1x

9.1 Overview

This chapter describes the IEEE 802.1x authentication method.

Port authentication is a way to validate access to ports on the Switch to clients based on an external server (authentication server). The Switch supports the following method for port authentication:

- **IEEE 802.1x**[1] - An authentication server validates access to a port based on a username and password provided by the user.

IEEE 802.1x authentication uses the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See Section 9.6 on page 71 for more information on configuring your RADIUS server settings.

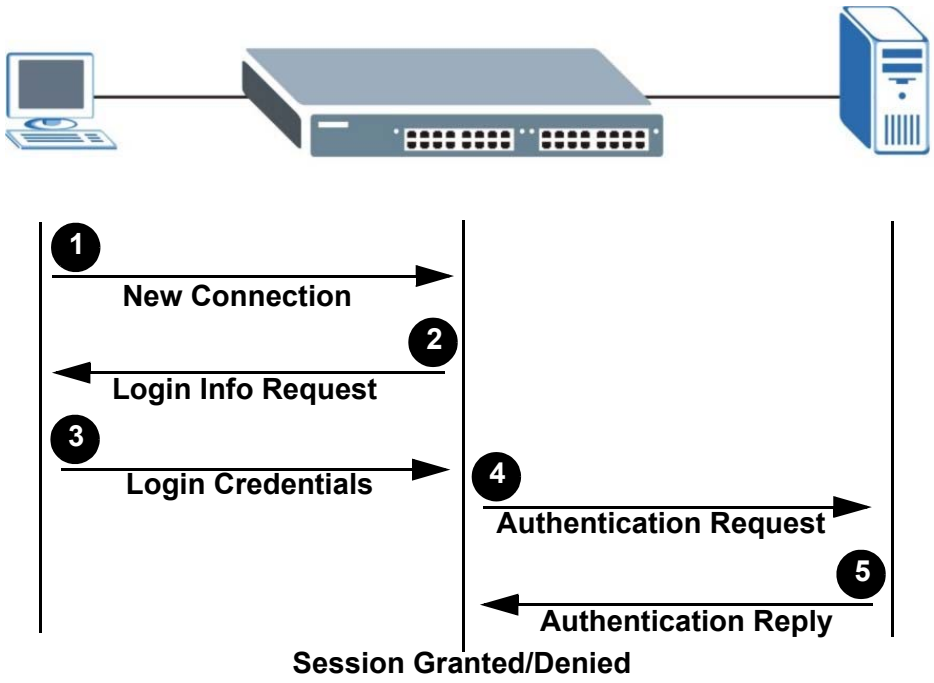
9.1.1 IEEE 802.1x Authentication

The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password. When the client provides the login credentials, the Switch sends an authentication

1. At the time of writing, IEEE 802.1x is not supported by all operating systems. See your operating system documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

Figure 30 IEEE 802.1x Authentication Process



9.1.2 Guest VLAN

When 802.1x port authentication is enabled on the Switch, clients that do not have the correct credentials are blocked from using the port(s). You can configure your Switch to have one Guest VLAN. Traffic coming from the Guest VLAN are directed to the Guest network and can have access to unrestricted areas of the network, such as the Internet. The rights granted to the Guest VLAN depends on how the network administrator configures switches or routers with the Guest network feature.

Note: Use the Switch to assign the Guest VLAN to a port. This assignment should corresponds to the network's Guest VLAN. The Guest network is not configurable in this Switch.

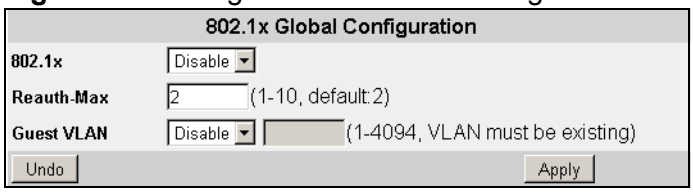
To enable port authentication, first activate the port authentication method (both on the Switch and the port(s)) then configure the RADIUS server settings in the **Radius Server Configuration** screen (Section 9.4 on page 68).

9.2 802.1x Global Configuration Screen

Use this screen to enable port authentication and a guest VLAN on the Switch.

Click **Configuration > 802.1x > Global Configuration** in the navigation panel to display the screen as shown.

Figure 31 Configuration > Global Configuration



The following table describes the labels in this screen.

Table 14 Configuration > Global Configuration

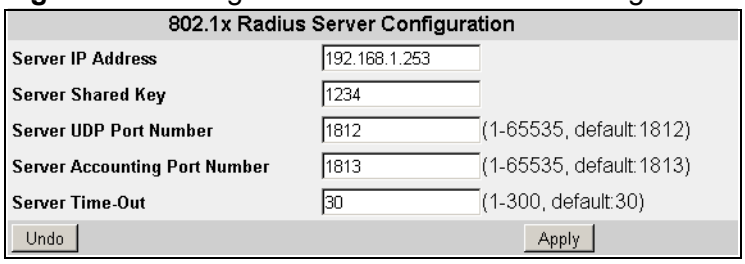
LABEL	DESCRIPTION
802.1x	Select **Enable** to activate the port authentication method on the Switch. Otherwise, select **Disable**.
Reauth-Max	Specify the number of times the Switch tries to authenticate client(s) before sending unresponsive ports to the Guest VLAN. This is set to **2** by default. That is, the Switch attempts to authenticate a client twice. If the client does not respond to the first authentication request, the Switch tries again. If the client still does not respond to the second request, the Switch sends the client to the Guest VLAN. The client needs to send a new request to be authenticated by the Switch again.
Guest VLAN	Select **Enable** then enter the number that identifies the Guest VLAN. Make sure this is the Guest VLAN recognized in your network. Clients belonging to the guest VLAN can access unprotected areas in your network, such as the Internet. Select **Disable** if you do not want to use this feature.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

9.3 802.1x Radius Server Configuration Screen

Use this screen to configure the RADIUS server settings.

Click **Configuration > 802.1x > Radius Server Configuration** in the navigation panel to display the screen as shown.

Figure 32 Configuration > Radius Server Configuration



The following table describes the labels in this screen.

Table 15 Configuration > Radius Server Configuration

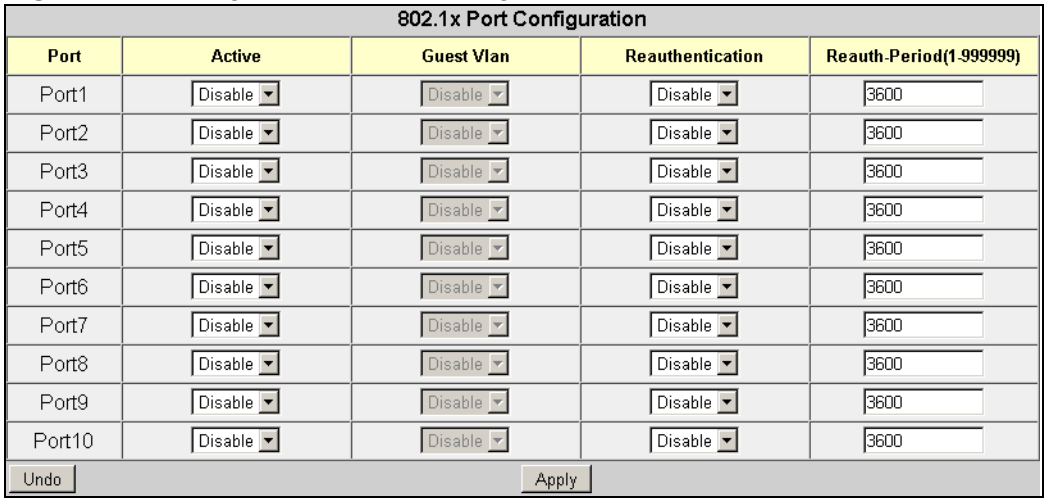
LABEL	DESCRIPTION
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Server Shared Key	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external authentication server and the Switch. The key must be the same on the external authentication server and your Switch. The key is not sent over the network.
Server UDP Port Number	Enter the port number of the RADIUS server. The default port number is 1812.
Server Accounting Port Number	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Server Time Out	Type how many minutes a session can be left idle before the session times out.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

9.4 802.1x Port Configuration Screen

Use this screen to enable and configure port authentication on individual ports.

Click **Configuration > 802.1x > Port Configuration** in the navigation panel to display the screen as shown.

Figure 33 Configuration > Port Configuration



The following table describes the labels in this screen.

Table 16 Configuration > Port Configuration

LABEL	DESCRIPTION
Port	This field displays the port number.
Active	Select this check box to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Guest VLAN	You can configure this if you have enabled the guest VLAN feature in the **Configuration > Global Configuration** screen (see Section 9.2 on page 67). Select **Enable** then enter the number that identifies the Guest VLAN. Make sure this is the Guest VLAN recognized in your network. Clients belonging to the guest VLAN can access unprotected areas in your network, such as the Internet. Select **Disable** if you do not want to use this feature.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauth-Period (1-999999)	Specify how often (in minutes) a client has to re-enter his or her username and password to stay connected to the port. Default is **3600** minutes (or 1 hour).
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

9.5 802.1x Radius Server Configuration Screen

Use this screen to view a summary of port authentication settings on the Switch and in each individual ports.

Click **Configuration > 802.1x > 802.1x Status** in the navigation panel to display the screen as shown.

Figure 34 Configuration > 802.1x Status

802.1x Status										
802.1x	Disable									
Guest VLAN	Enable									
Reauth-Max	2									
Server IP Address	192.168.1.253									
Server Shared Key	1234									
Sever UDP Port Number	1812									
Server Accounting Port Number	1813									
Sever Time-Out	30									
	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8	Port9	Port10
	Y:Yes N:No A:Accepted									
Active	N	N	N	N	N	N	N	N	N	N
Guest Vlan	N	N	N	N	N	N	N	N	N	N
Reauthentication	N	N	N	N	N	N	N	N	N	N
Reauth-Period	3600	3600	3600	3600	3600	3600	3600	3600	3600	3600

The following table describes the labels in this screen.

Table 17 Configuration > 802.1x Status

LABEL	DESCRIPTION
802.1x	This shows if port authentication is enabled on the Switch.
Guest VLAN	This shows if a Guest VLAN is enabled on the Switch.
Reauth-Max	This shows the number of times the Switch attempts to authenticate clients for port access.
Server IP Address	This is the IP address of the RADIUS server.
Server Shared Key	This is the password shared between the external authentication server and the Switch.
Server UDP Port Number	This is the port number of the RADIUS server.
Server Accounting Port Number	This is the port number of the external accounting server.
Server Time-Out	This shows how many minutes a session can be idle before the session times out. When a session times out, the client has to send a new request to the server and be authenticated again.
The table below describes the settings for ports 1-10	
Active	This shows if port authentication is enabled on the port.

Table 17 Configuration > 802.1x Status (continued)

LABEL	DESCRIPTION
Guest VLAN	This shows if a Guest VLAN is enabled on the port.
Reauthentication	This shows if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauth-Period	This shows how often (in minutes) a client has to re-enter his or her username and password to stay connected to the port.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

9.6 Technical Reference

This section provides technical background information about the topics covered in this chapter.

9.6.1 RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

Table 18 RADIUS vs. TACACS+

	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the Switch) and the TACACS server is encrypted.

9.6.2 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication, and accounting elements in a user profile, which is stored on the RADIUS server. This appendix lists the RADIUS attributes supported by the Switch.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication. Refer to RFC 2866 and RFC 2869 for RADIUS attributes used for accounting.

This section lists the attributes used by authentication and accounting functions on the Switch. In cases where the attribute has a specific format associated with it, the format is specified.

9.6.3 Attributes Used for Authentication

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

9.6.3.1 Attributes Used for Authenticating Privilege Access

User-Name

- The format of the User-Name attribute is **$enab**#**$**, where # is the privilege level (1-14).

User-Password

NAS-Identifier

NAS-IP-Address

9.6.3.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

9.6.3.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

- This value is set to **Ethernet(15)** on the Switch.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

9.6.4 Attributes Used for Accounting

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

9.6.4.1 Attributes Used for Accounting System Events

NAS-IP-Address

NAS-Identifier

Acct-Status-Type

Acct-Session-ID

- The format of Acct-Session-Id is **date+time+8-digit sequential number**, for example, 200704191721030000000001. (date: 2007/04/19, time: 17:21:03, serial number: 00000001)

Acct-Delay-Time

9.6.4.2 Attributes Used for Accounting Exec Events

The attributes are listed in the following table along with the time that they are sent (the difference between Console and Telnet/SSH Exec events is that the Telnet/SSH events utilize the Calling-Station-Id attribute):

Table 19 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-IP-Address	Y	Y	Y
Service-Type	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Session-Time		Y	Y
Acct-Terminate-Cause			Y

Table 20 RADIUS Attributes - Exec Events via Telnet/SSH

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-IP-Address	Y	Y	Y
Service-Type	Y	Y	Y
Calling-Station-Id	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y

Table 20 RADIUS Attributes - Exec Events via Telnet/SSH

ATTRIBUTE	START	INTERIM-UPDATE	STOP
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Session-Time		Y	Y
Acct-Terminate-Cause			Y

9.6.4.3 Attributes Used for Accounting IEEE 802.1x Events

The attributes are listed in the following table along with the time of the session they are sent:

Table 21 RADIUS Attributes-Exec Events via 802.1x

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-IP-Address	Y	Y	Y
NAS-Port	Y	Y	Y
Class	Y	Y	Y
Called-Station-Id	Y	Y	Y
Calling-Station-Id	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-Port-Type	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Input-Octets		Y	Y
Acct-Output-Octets		Y	Y
Acct-Session-Time		Y	Y
Acct-Input-Packets		Y	Y
Acct-Output-Packets		Y	Y
Acct-Terminate-Cause			Y
Acct-Input-Gigawords		Y	Y
Acct-Output-Gigawords		Y	Y

10 Bridge

10.1 Overview

The Switch supports Rapid Spanning Tree Protocol (RSTP) as defined in the IEEE 802.1w Rapid Spanning Tree Protocol standard.

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge that then notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this user's guide, "STP" refers to both STP and RSTP.

10.1.1 STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 22 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535

Table 22 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

10.1.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network frames are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

10.1.3 STP Port States

STP assigns five port states to eliminate frame looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

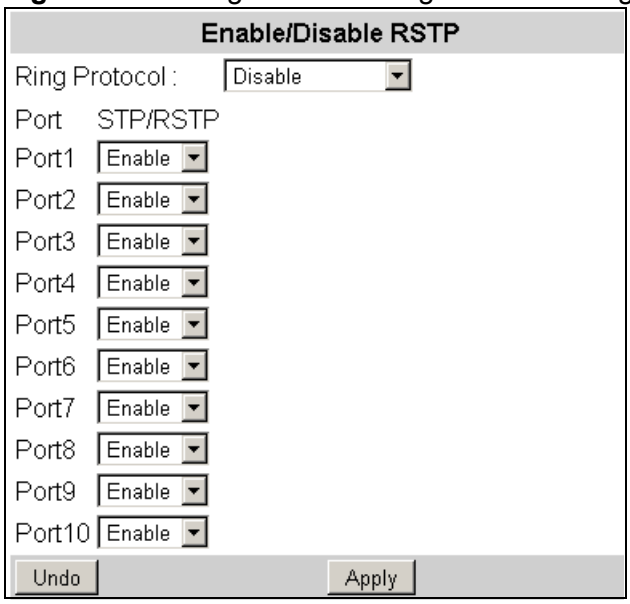
Table 23 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

10.2 The Bridge Configuration Screen

Click **Configuration** > **Bridge Menu** > **Bridge Config** to open the following screen.

Figure 35 Configuration > Bridge Menu > Bridge Config



The following table describes the labels in this screen.

Table 24 Configuration > Bridge Menu > Bridge Config

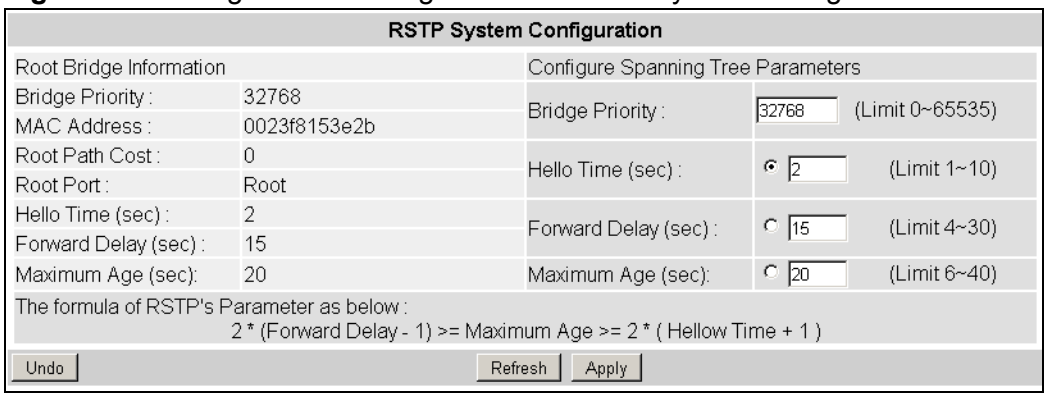
LABEL	DESCRIPTION
Ring Protocol	Select **RSTP (802.1W)** to enable RSTP. Select **Disable** if you do not want to use this feature.
Port	Select **Enable** to have the port participate in RSTP when you select **RSTP (802.1W)** in the **Ring Protocol** field. Select **Disable** so that the port will not participate in RSTP when you select **RSTP (802.1W)** in the Ring Protocol field. Select **Tunnel** so that the port will not participate in RSTP. When the tunnel port receives Bridge Protocol Data Units (BPDU) frames, the Switch forwards the frames to other tunnel ports.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

10.3 The RSTP System Configuration Screen

You must first enable RSTP in the **Bridge Configuration** screen in order to open this screen.

Click **Configuration** > **Bridge Menu** > **RSTP System Config** to open the following screen.

Figure 36 Configuration > Bridge Menu > RSTP System Config


RSTP System Configuration
Root Bridge Information
Bridge Priority : 32768
MAC Address : 0023f8153e2b
Root Path Cost : 0
Root Port : Root
Hello Time (sec) : 2
Forward Delay (sec) : 15
Maximum Age (sec): 20
Configure Spanning Tree Parameters
Bridge Priority : 32768 (Limit 0~65535)
Hello Time (sec) : 2 (Limit 1~10)
Forward Delay (sec) : 15 (Limit 4~30)
Maximum Age (sec): 20 (Limit 6~40)
The formula of RSTP's Parameter as below :
2 * (Forward Delay - 1) >= Maximum Age >= 2 * (Hellow Time + 1)
Undo
Refresh
Apply

The following table describes the labels in this screen.

Table 25 Configuration > Bridge Menu > RSTP System Config

LABEL	DESCRIPTION
Root Bridge Information	
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
MAC Address	This is the root bridge's MAC address.
Root Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see Table 22 on page 75 for more information.
Root Port	This shows whether the Switch connects to another root switch (through port number **1-10**) or serves as a root switch (**Root**).
Hello Time (sec)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Forward Delay (sec)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
Max age (sec)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Configuration Spanning Tree Parameters	
RSTP Force Version	Use this to force the spanning tree algorithm to run on either the **STP** or **RSTP** protocol.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time (sec)	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

Table 25 Configuration > Bridge Menu > RSTP System Config

LABEL	DESCRIPTION
Forward Delay (sec)	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Max age (sec)	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Undo	Click this to restore your last saved settings.
Refresh	Click this to reset the data for the field(s).
Apply	Click this to save your changes.

10.4 The Spanning Tree Port Configuration

Click **Configuration** > **Bridge Menu** > **RSTP Per Port Config** to open the following screen.

Figure 37 Configuration > Bridge Menu > RSTP Per Port Config

Spanning Tree Port Configuration

Port	Type	Priority (1~255)	Cost (1~65535)	Edge	P2P	Port Status	Port Role
1	RJ45	128	19	On	Auto	Forwarding	Designated
2	RJ45	128	19	On	Auto	Blocking	Disabled
3	RJ45	128	19	On	Auto	Blocking	Disabled
4	RJ45	128	19	On	Auto	Blocking	Disabled
5	RJ45	128	19	On	Auto	Blocking	Disabled
6	RJ45	128	19	On	Auto	Blocking	Disabled
7	RJ45	128	19	On	Auto	Blocking	Disabled
8	RJ45	128	19	On	Auto	Blocking	Disabled
9	Fiber	128	4	Off	Auto	Blocking	Disabled
10	Fiber	128	4	Off	Auto	Blocking	Disabled

Undo Apply

The following table describes the labels in this screen.

Table 26 Configuration > Bridge Menu > RSTP Per Port Config

LABEL	DESCRIPTION
Port	This is the port index number.
Type	This is the cable type connected to the port.
Priority (1~255)	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Cost (1~65535)	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost-see Table 22 on page 75 for more information.
Edge	Select **On** when the port is connected to an end node (a computer network card for example). Select **Off** when the port is connected to a bridge node.
P2P	Select **On** when the port is connected to one bridge as a Point-to-Point link type. Select **Off** when the port is connected to multiple bridges as a Shared Medium link type. Select **Auto** to have the Switch automatically determine the link type.
Port Status	This shows whether the port is **Forwarding** or **Blocking** frame transmission.
Port Role	This shows the port behavior as a **Disabled**, **Alternate**, **Backup**, **Root**, **Designated** or **NonStp** port.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

11 VLAN

11.1 Overview

This chapter shows you how to configure 802.1Q tagged and port-based VLANs. A VLAN (Virtual Local Area Network) is a network that is not limited by the physical location of a device (such as a switch).

11.2 Introduction to IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 bits

11.2.1 Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

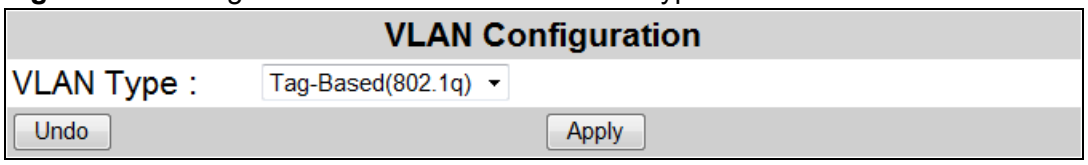
Table 27 IEEE 802.1Q VLAN Terminology

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/ deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.
	Ingress filtering	If set, the Switch discards incoming frames for VLANs that do not have this port as a member.

11.3 The VLAN Type Screen

Use this screen to select the VLAN type. Click **Configuration** > **VLAN Menu** > **VLAN Type** to open the following screen.

Figure 38 Configuration > VLAN Menu > VLAN Type



The following table describes the labels in this screen.

Table 28 Configuration > VLAN Menu > VLAN Type

LABEL	DESCRIPTION
VLAN Type	Use this to set the Switch to **Port-Based** or **Tag-Based(802.1q)** VLAN mode.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

11.4 The Port-Based VLAN Screen

Port-based VLANs are VLANs where the frame forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data frame leaves) for both ports.

Port-based VLANs are specific only to the Switch on which they were created.

This screen is available only when you select **Port-Based** in the **VLAN Type** screen. Click **Configuration** > **VLAN Menu** > **Port-Based** to open the following screen.

Figure 39 Configuration > VLAN Menu > Port-Based

Port-Based VLAN Configuration

Port Number	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8	Port9	Port10	Switch Management
Port 1	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Enable

Apply

Port-Based VLAN Status

Port Number	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8	Port9	Port10	Switch Management
Port1	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Enable
Port2	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Enable
Port3	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Enable
Port4	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Enable
Port5	Y	Y	Y	Y	-	Y	Y	Y	Y	Y	Enable
Port6	Y	Y	Y	Y	Y	-	Y	Y	Y	Y	Enable
Port7	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	Enable
Port8	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Enable
Port9	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Enable
Port10	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Enable

The following table describes the labels in this screen.

Table 29 Configuration > VLAN Menu > Port-Based

LABEL	DESCRIPTION
Port-Based VLAN Configuration	
Port Number	Use this to select the port you are configuring.
Port1-10	Select the subscriber ports that can talk to each other.
Switch Management	Use this to enable or disable switch management via the web configurator, Telnet or SNMP manager. Select the port through which you can manage the Switch. If you disable this feature, then you cannot access the web configurator from a computer connected to this port.
Apply	Click this to save your changes.
Port-Based VLAN Status	
Port Number	This is the port number.
Port1-10	This shows the subscriber ports that can talk to each other.
Switch Management	This shows whether switch management is enabled or disabled.

11.5 The Tag-Based VLAN Screens

Use the **Tag-Based VLAN** screens to configure VLAN settings.

11.5.1 VLAN Stacking

A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.

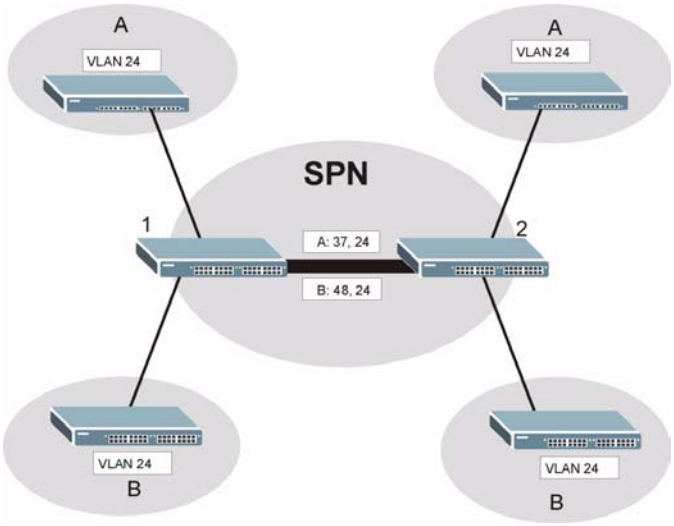
A service provider's customers may require a range of VLANs to handle multiple applications. A service provider's customers can assign their own inner VLAN tags on ports for these applications. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

11.5.2 VLAN Stacking Example

In the following example figure, both **A** and **B** are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to

distinguish customer **A** and tag 48 to distinguish customer **B** at edge device **1** and then stripping those tags at edge device **2** as the data frames leave the network.

Figure 40 VLAN Stacking Example



11.5.3 VLAN Stacking Port Roles

Each port can have three VLAN stacking "roles", **Normal**, **Access Port** and **Tunnel** (the latter is for Gigabit ports only).

Note: Some devices do not support all roles.

- Select **Normal** for "regular" (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access Port** for ingress ports on the service provider's edge devices (**1** and **2** in the VLAN stacking example figure). The incoming frame is treated as "untagged", so a second VLAN tag (outer VLAN tag) can be added.

Note: Static VLAN **Tx Tagging** MUST be disabled on a port where you choose **Normal** or **Access Port**.

- Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by SP VID).

Note: Static VLAN **Tx Tagging** MUST be enabled on a port where you choose **Tunnel Port**.

11.5.4 VLAN Tag Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

Table 30 VLAN Tag Format

Type	Priority	VID

Type is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. **SP TPID** (Service Provider Tag Protocol Identifier) is the service provider VLAN stacking tag type. Many vendors use 0x8100 or 0x9100.

TPID (Tag Protocol Identifier) is the customer IEEE 802.1Q tag.

- If the VLAN stacking port role is **Access**, then the Switch adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure).
- If the VLAN stacking port role is **Tunnel**, then the Switch only adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure) that have an **SP TPID** different to the one configured on the Switch. (If an incoming frame's **SP TPID** is the same as the one configured on the Switch, then the Switch will not add the tag.)

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for.

- On the Switch, configure priority level of inner IEEE 802.1Q tag in the **Configuration** > **QoS Menu** > **802.1p Priority** screen.
- "0" is the lowest priority level and "7" is the highest.

VID is the VLAN ID. **SP VID** is the VID for the second (service provider's) VLAN tag.

11.5.5 Frame Format

The frame format for an untagged Ethernet frame, a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) is shown next.

Configure the fields as highlighted in the Switch **VLAN Stacking** screen.

Table 31 Single and Double Tagged 802.11Q Frame Format

						DA	SA	Len/ Etype	Data	FCS	Untagged Ethernet frame
			DA	SA	**TPID**	**Priority**	**VID**	Len/ Etype	Data	FCS	IEEE 802.1Q customer tagged frame
DA	SA	**SPTPID**	**Priority**	**VID**	**TPID**	**Priority**	**VID**	Len/ Etype	Data	FCS	Double-tagged frame

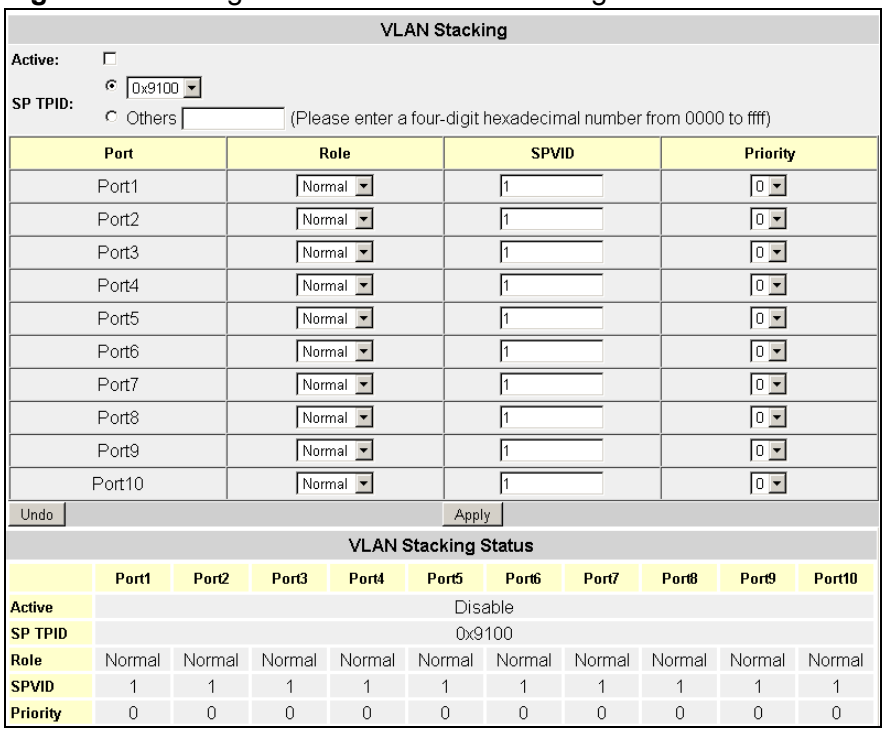
Table 32 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/ Etype	Length and type of Ethernet frame
(SP)TPID	(Service Provider) Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

11.5.6 The VLAN Stacking Configuration Screen

Use this screen to enable VLAN stacking on the Switch. Click **Configuration** > **VLAN Menu** > **Tag-Based** > **VLAN Stacking** to open the following screen.

Figure 41 Configuration > VLAN Menu > Tag-Based > VLAN Stacking



The following table describes the labels in this screen.

Table 33 Configuration > VLAN Menu > Tag-Based > VLAN Stacking

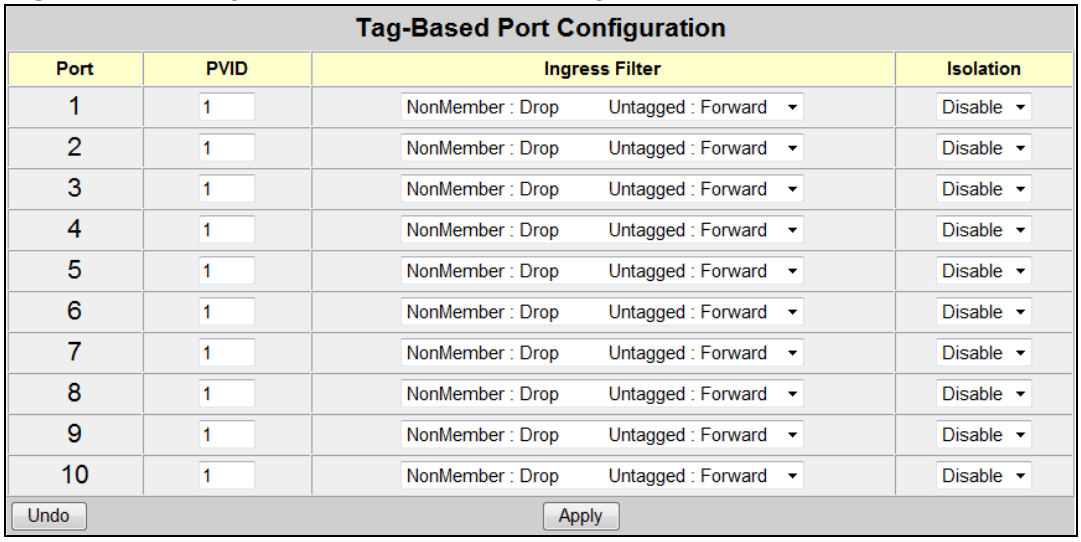
LABEL	DESCRIPTION
VLAN Stacking	
Active	Select this to enable VLAN stacking on the Switch.
SP TPID	**SP TPID** is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. Choose **0x8100** or **0x9100** from the drop-down list box or select **Others** and then enter a four-digit hexadecimal number from 0x0000 to 0xFFFF. 0x denotes a hexadecimal number. It does not have to be typed in the **Others** text field.
Port	The port number identifies the port you are configuring.
Role	Select **Access** to have the Switch add the **SP TPID** tag to all incoming frames received on this port. Select **Access Port** for ingress ports at the edge of the service provider's network. Select **Tunnel** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.
SPVID	**SPVID** is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port.
Priority	On the Switch, configure priority level of inner IEEE 802.1Q tag in the **Configuration** > **QoS Menu** > **802.1p Priority** screen. "0" is the lowest priority level and "7" is the highest.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.
VLAN Stacking Status	
Port1-10	This is the port number.
Active	This shows whether VLAN stacking is enabled or disabled on the Switch.
SP TPID	This is the service provider VLAN tag.
Role	This shows how the port process transmitted frames.
SPVID	This is the service provider ID for frames received on this port.
Priority	This shows the priority level of frames transmitted through the port.

11.5.7 The Tag-Based Port Information Screen

Use this screen to configure how the Switch handles incoming traffic passing through the port.

Click **Configuration** > **VLAN Menu** > **Tag-Based** > **Port Info.** to open the following screen.

Figure 42 Configuration > VLAN Menu > Tag-Based > Port Info.


Tag-Based Port Configuration
Port
PVID
Ingress Filter
Isolation
1 1 NonMember : Drop Untagged : Forward Disable
2 1 NonMember : Drop Untagged : Forward Disable
3 1 NonMember : Drop Untagged : Forward Disable
4 1 NonMember : Drop Untagged : Forward Disable
5 1 NonMember : Drop Untagged : Forward Disable
6 1 NonMember : Drop Untagged : Forward Disable
7 1 NonMember : Drop Untagged : Forward Disable
8 1 NonMember : Drop Untagged : Forward Disable
9 1 NonMember : Drop Untagged : Forward Disable
10 1 NonMember : Drop Untagged : Forward Disable
Undo
Apply

The following table describes the labels in this screen.

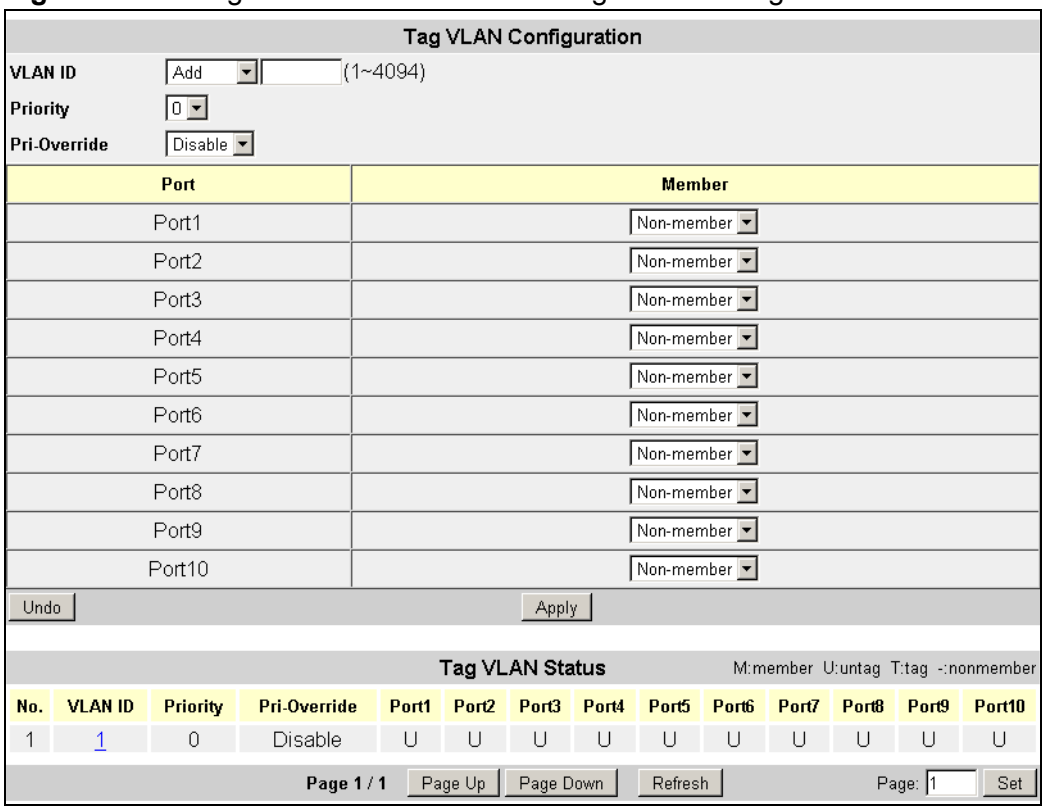
Table 34 Configuration > VLAN Menu > Tag-Based > Port Info.

LABEL	DESCRIPTION
Port	This is the port index number.
PVID	Enter a number between 1 and 4094 as the port VLAN ID.
Ingress Filter	Use this to determine the action about incoming traffic passing through the port. • **NonMember: Forward, Untagged: Forward**: Forward frames that do not belong to any VLAN group and forward untagged VLAN frames. • **NonMember: Drop, Untagged: Forward**: Drop frames that do not belong to any VLAN group and forward untagged VLAN frames. • **NonMember: Drop, Untagged: Drop**: Drop frames that do not belong to any VLAN group and drop untagged VLAN frames.
Isolation	Use this to enable or disable port isolation. Port isolation allows each port to communicate only with the management port but not communicate with each other. This option is the most limiting but also the most secure.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

11.5.8 The Tag-Based Port Configuration Screen

Use this screen to configure the VLAN group settings for each port on the Switch. Click **Configuration** > **VLAN Menu** > **Tag-Based** > **Tag-Based info.** to open the following screen.

Figure 43 Configuration > VLAN Menu > Tag-Based > Tag-Based info.



The following table describes the labels in this screen.

Table 35 Configuration > VLAN Menu > Tag-Based > Tag-Based info.

LABEL	DESCRIPTION
VLAN ID	Select whether you want to **Add** or **Modify** a VLAN ID. Enter the VLAN ID from 1-4094 that you want to configure.
Priority	This is the priority you want to assign to the tag-based VLAN.
Pri-Override	Select **Enable** to ignore the priority level assigned to the transmitted frames. Otherwise, select **Disable**.
Port	This shows ports 1 to 10.
Member	This shows the VLAN group setting for the port, whether it is a **Member**, **Untagging**, **Tagging** or **Non-member**.
Undo	Click this to reset the values in this screen to their last-saved values.
Apply	Click this to save your changes.
Tag VLAN Status (M:member U:untag T:tag)	

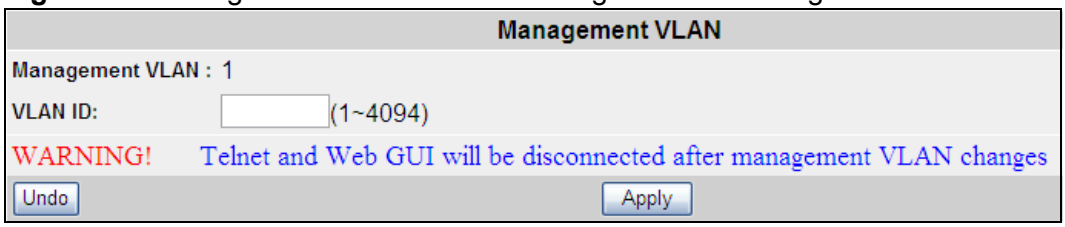
Table 35 Configuration > VLAN Menu > Tag-Based > Tag-Based info.

LABEL	DESCRIPTION
Add VLAN Configuration	
VLAN ID	Enter a VLAN ID number from 1 to 4094.
Priority	This is the priority you want to assign to the Tag-based VLAN.
Pri-Override	Select **Enable** to ignore the priority level assigned to the transmitted frames. Otherwise, select **Disable**.
Port 1-10	A **Member** port is a permanent member of this VLAN group. An **Untagging** port strips off the 802.1Q tag from incoming and outgoing frames. Use this to send untag frames to devices that do no support the 802.1Q feature. A **Tagging** port tags incoming and outgoing frames with this VLAN group information. A **Non-member** port does not participate in the VLAN group.
Page Up	Click this to view the next page.
Page Down	Click this to view the previous page.
Refresh	Click this to refresh the screen.
Page... Set	Enter a page number and click Set to go to that page.

11.5.9 The Management VLAN Screen

Use this to configure the management VLAN. A port must belong to the management VLAN if you want to access the Switch's web configurator via that port. Click **Configuration** > **VLAN Menu** > **Tag-Based** > **Management VLAN** to open the following screen.

Figure 44 Configuration > VLAN Menu > Tag-Based > Management VLAN



The following table describes the labels in this screen.

Table 36 Configuration > VLAN Menu > Tag-Based > Management VLAN

LABEL	DESCRIPTION
Management VLAN	This is the current management VLAN.
VLAN ID	Enter an ID number from 1 to 4094. 1 is the default value. If you change this, you will be disconnected from the web configurator unless your current access belongs to the new VLAN.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

12

Bandwidth Control

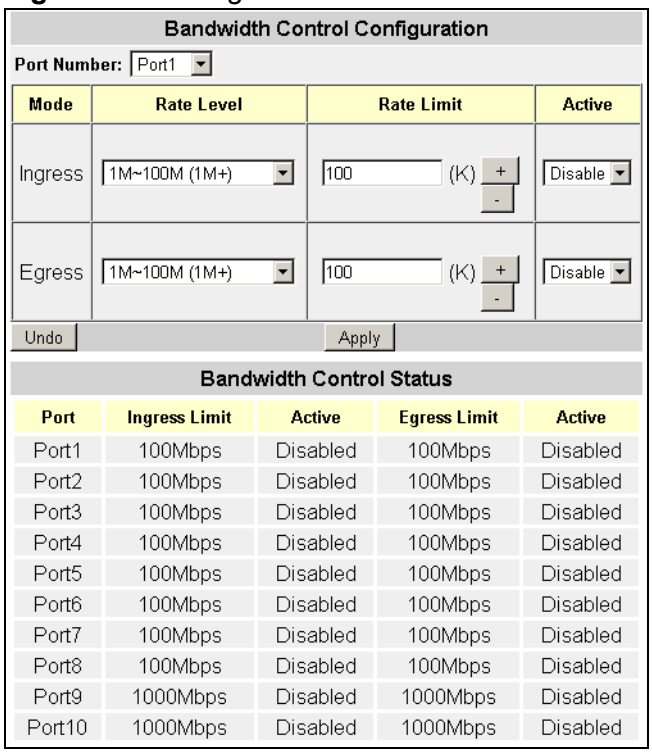
12.1 Overview

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.

12.2 Bandwidth Control Setup

Click **Configuration** > **Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 45 Configuration > Bandwidth Control



Bandwidth Control Configuration

Port Number: Port1

Mode	Rate Level	Rate Limit	Active
Ingress	1M~100M (1M+)	100 (K) + -	Disable
Egress	1M~100M (1M+)	100 (K) + -	Disable

Undo Apply

Bandwidth Control Status

Port	Ingress Limit	Active	Egress Limit	Active
Port1	100Mbps	Disabled	100Mbps	Disabled
Port2	100Mbps	Disabled	100Mbps	Disabled
Port3	100Mbps	Disabled	100Mbps	Disabled
Port4	100Mbps	Disabled	100Mbps	Disabled
Port5	100Mbps	Disabled	100Mbps	Disabled
Port6	100Mbps	Disabled	100Mbps	Disabled
Port7	100Mbps	Disabled	100Mbps	Disabled
Port8	100Mbps	Disabled	100Mbps	Disabled
Port9	1000Mbps	Disabled	1000Mbps	Disabled
Port10	1000Mbps	Disabled	1000Mbps	Disabled

The following table describes the related labels in this screen.

Table 37 Configuration > Bandwidth Control

LABEL	DESCRIPTION
Bandwidth Control Configuration	
Port Number	Use this to select a port number.
Mode	This shows the **Ingress** (incoming) or **Egress** (outgoing) mode.
Rate Level	Select a rate range from the list. Options are: 64K~960K (64+), 1M~100M (1M+), 110M~1000M (10M+).
Rate Limit	Specify the maximum bandwidth allowed for the traffic flow on a port. The unit changes depending on how you configure in the **Rate Level** field. The value you enter in this field must be within the rate level range.
Active	Use this to enable or disable bandwidth control.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.
Bandwidth Control Status	
Port	This is the port number.
Ingress Limit	This is the ingress rate limit on the port.
Active	This shows whether bandwidth control for ingress traffic is enabled or disabled on the port.
Egress Limit	This is the egress rate limit on the port.
Active	This shows whether bandwidth control for egress traffic is enabled or disabled on the port.

13

Broadcast Storm Control

13.1 Overview

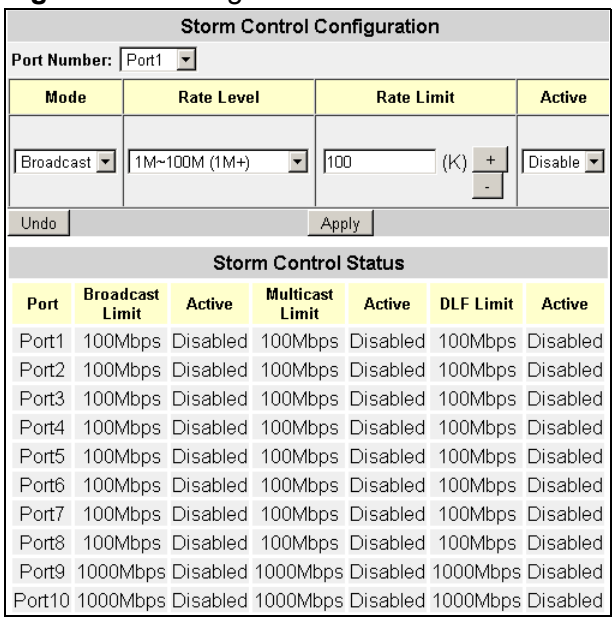
This chapter introduces and shows you how to configure the broadcast storm control feature.

13.2 Broadcast Storm Control Setup

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) frames the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF frames is reached per second, the subsequent frames are discarded. Enable this feature to reduce broadcast, multicast and/or DLF frames in your network. You can specify limits for each frame type on each port.

Click **Configuration** > **Storm Control** in the navigation panel to display the screen as shown next.

Figure 46 Configuration > Storm Control



Storm Control Configuration

Port Number: Port1

Mode	Rate Level	Rate Limit	Active
Broadcast	1M~100M (1M+)	100 (K) + -	Disable

Undo Apply

Storm Control Status

Port	Broadcast Limit	Active	Multicast Limit	Active	DLF Limit	Active
Port1	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port2	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port3	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port4	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port5	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port6	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port7	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port8	100Mbps	Disabled	100Mbps	Disabled	100Mbps	Disabled
Port9	1000Mbps	Disabled	1000Mbps	Disabled	1000Mbps	Disabled
Port10	1000Mbps	Disabled	1000Mbps	Disabled	1000Mbps	Disabled

The following table describes the labels in this screen.

Table 38 Configuration > Storm Control

LABEL	DESCRIPTION
Storm Control Configuration	
Port Number	Use this to select a port number.
Mode	Select the **Broadcast**, **Multicast** or **DLF** mode from the list.
Rate Level	Select a rate range from the list. Options are: 64K~960K (64+), 1M~100M (1M+), 110M~1000M (10M+).
Rate Limit	Specify specify how many frames the port receives per second. The unit changes depending on how you configure in the **Rate Level** field. The value you enter in this field must be within the rate level range.
Active	Use this to enable or disable storm control.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.
Storm Control Status	
Port	This is the port number.
Broadcast Limit	This is the broadcast frame limit on the port.
Active	This shows whether broadcast control is enabled or disabled on the port.
Multicast Limit	This is the multicast frame limit on the port.
Active	This shows whether multicast control is enabled or disabled on the port.
DLF Limit	This is the Destination Lookup Failure (DLF) frame limit on the port.
Active	This shows whether DLF control is enabled or disabled on the port.

14

Port Mirroring

14.1 Overview

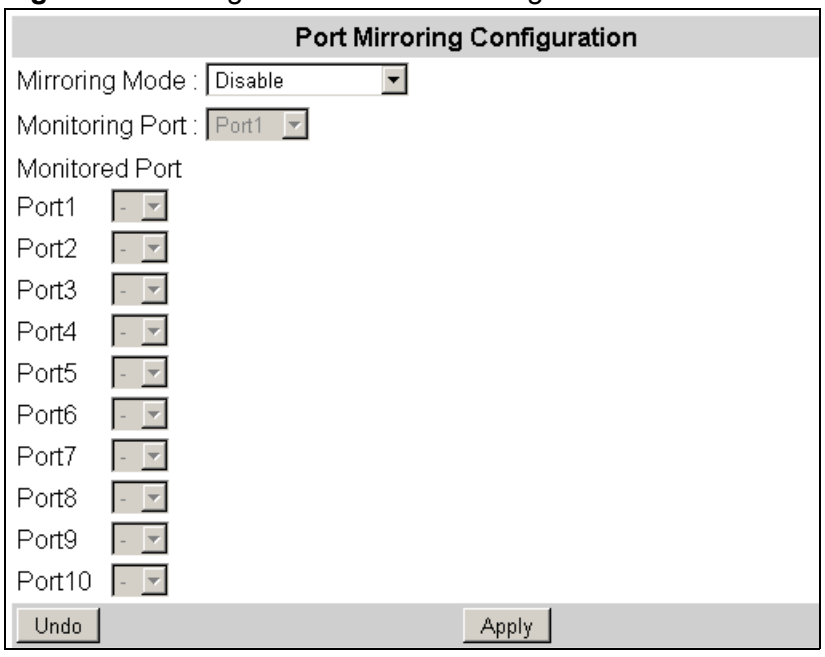
This chapter discusses port mirroring setup screens.

14.2 Port Mirroring Setup

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

Click **Configuration > Port Mirroring** in the navigation panel to display the following screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 47 Configuration > Port Mirroring



The following table describes the labels in this screen.

Table 39 Configuration > Port Mirroring

LABEL	DESCRIPTION
Mirroring Mode	Use this to enable or disable the port mirroring feature. The active port mirroring feature monitors both incoming and outgoing traffic.
Monitoring Port	The monitoring port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Select the monitor port number from the list.
Monitored Port	Select the port(s) to mirror the traffic on a port.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

15

Link Aggregation

15.1 Overview

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group.

The Switch supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

See Section 15.3 on page 102 for a static port trunking example.

15.2 Dynamic Link Aggregation

The Switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The Switch supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregation Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the "standby" ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

15.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information[2]:

Table 40 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

Table 41 Link Aggregation ID: Peer Switch

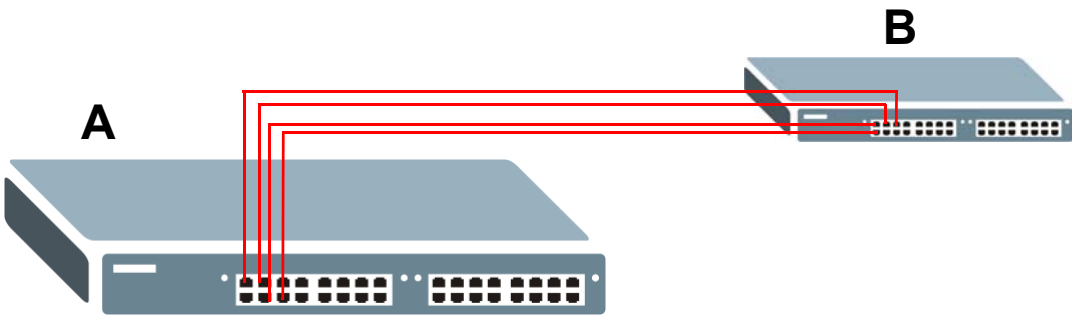
SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

15.3 Static Trunking Example

This example shows you how to create a static port trunk group for ports 2-5.

1 **Make your physical connections** - make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows ports 2-5 on switch **A** connected to switch **B**.

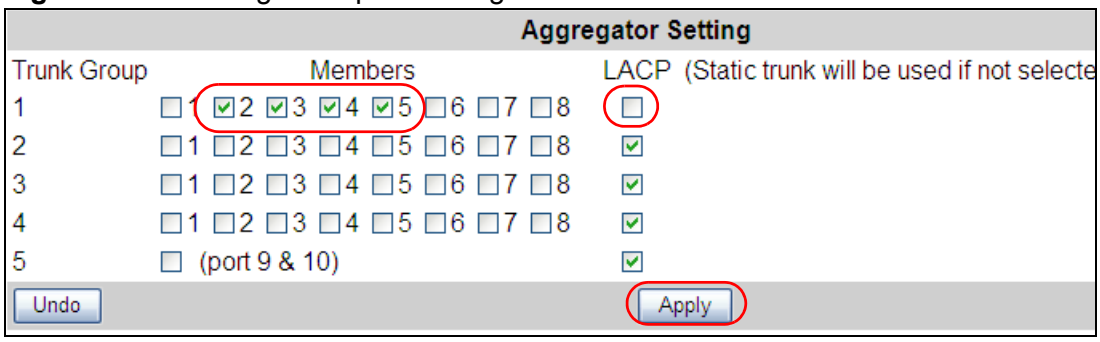
Figure 48 Trunking Example - Physical Connections



2. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

2 **Configure static trunking**-Click **Configuration** > **Trunk Config** > **Aggregator Setting**. In this screen select the ports that should belong to trunk group 1 as shown in the figure below. Do not select the **LACP** option. Click **Apply** when you are done.

Figure 49 Trunking Example - Configuration Screen

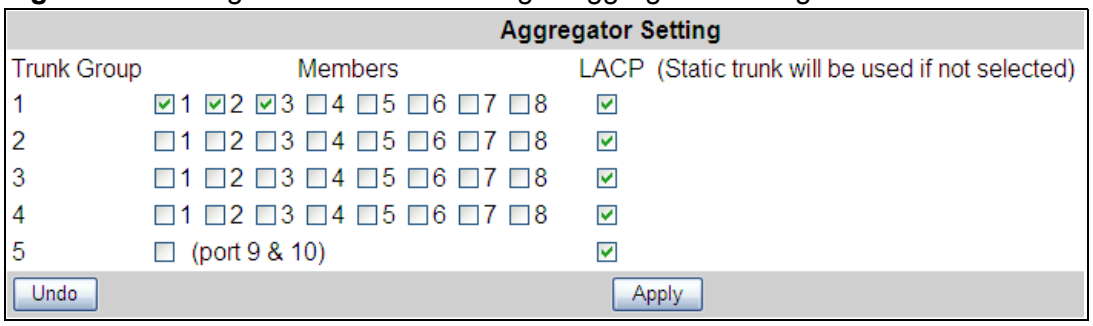


Your trunk group 1 configuration is now complete; you do not need to go to any additional screens.

15.4 Link Aggregation Setting

Click **Configuration** > **Trunk Config > Aggregator Setting** to display the screen shown next. See Section 15.1 on page 101 for more information on link aggregation.

Figure 50 Configuration > Trunk Config > Aggregator Setting



The following table describes the labels in this screen.

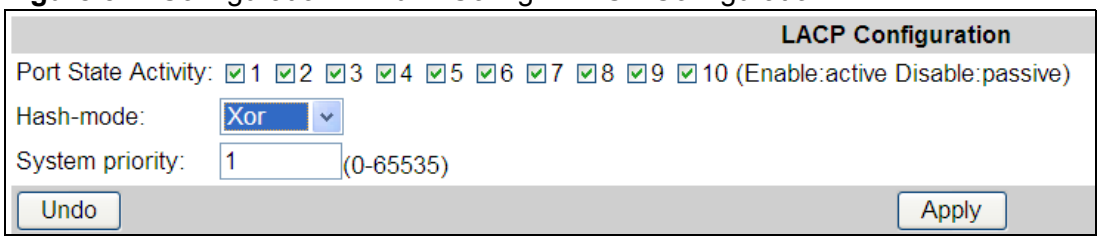
Table 42 Configuration > Trunk Config > Aggregator Setting

LABEL	DESCRIPTION
Group	This is the trunk group index number. The Switch supports up to four trunk groups for 100Mbps ports and up to two trunk groups for Gigabit ports. 100Mbps ports and Gigabit ports cannot be in the same group.
Members	Select the port(s) that belong to a trunk group. For Groups 1 to 4, you can select up to four port members for each group. For Group 5, you can select the two Gigabit ports as the members.
LACP	Use this to enable or disable LACP port trunking.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

15.5 Link Aggregation Control Protocol

Click **Configuration** > **Trunk Config** > **LACP Configuration** to display the screen shown next. See Section 15.2 on page 101 for more information on dynamic link aggregation.

Figure 51 Configuration > Trunk Config > LACP Configuration


LACP Configuration
Port State Activity: 1 2 3 4 5 6 7 8 9 10 (Enable:active Disable:passive)
Hash-mode: Xor
System priority: 1 (0-65535)
Undo
Apply

The following table describes the labels in this screen.

Table 43 Configuration > Trunk Config > LACP Configuration

LABEL	DESCRIPTION
Port State Activity	Select the port to enable Link Aggregation Control Protocol (LACP).
Hash-mode	Use this to specify the outgoing traffic distribution type. Select **Lookup** to distribute frames based on the destination MAC address. Select **Xor** to distribute frames based on the last 3 bits of the source MAC address and the trunk mask load balancing table.

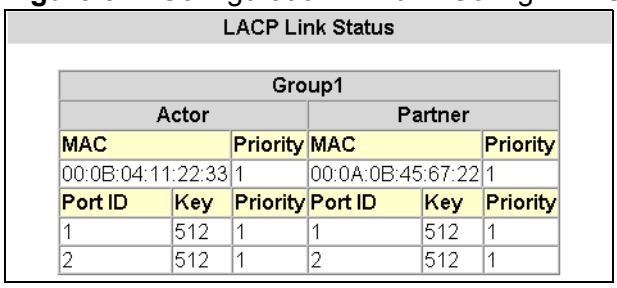
Table 43 Configuration > Trunk Config > LACP Configuration (continued)

LABEL	DESCRIPTION
System Priority	LACP system priority is a number between 1 and 65535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

15.6 LACP Link Status

Click **Configuration** > **Trunk Config > LACP Link Status** in the navigation panel to open the following screen.

Figure 52 Configuration > Trunk Config > LACP Link Status


LACP Link Status

Group1					
Actor			Partner		
MAC		Priority	MAC		Priority
00:0B:04:11:22:33		1	00:0A:0B:45:67:22		1
Port ID	Key	Priority	Port ID	Key	Priority
1	512	1	1	512	1
2	512	1	2	512	1

The following table describes the labels in this screen.

Table 44 Configuration > Trunk Config > LACP Link Status

LABEL	DESCRIPTION
Actor	This is the local Switch.
MAC	This is the local Switch's MAC address.
Priority	This is the local Switch's priority level.
Port ID	This shows the port number belonging to the trunk group.
Key	This is the local Switch's key value.
Priority	This is the port priority level.
Partner	This is the peer Switch.
MAC	This is the peer Switch's MAC address.
Priority	This is the peer Switch's priority level.
Port ID	This shows the port number belonging to the trunk group.
Key	This is the peer Switch's key value.
Priority	This is the port priority level.

16 IGMP

16.1 Overview

Traditionally, IP frames are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP frames to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

16.1.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send frames to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

16.1.2 IGMP Snooping

A Switch can passively snoop on IGMP frames transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP frames passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

16.1.3 IGMP Snooping and VLANs

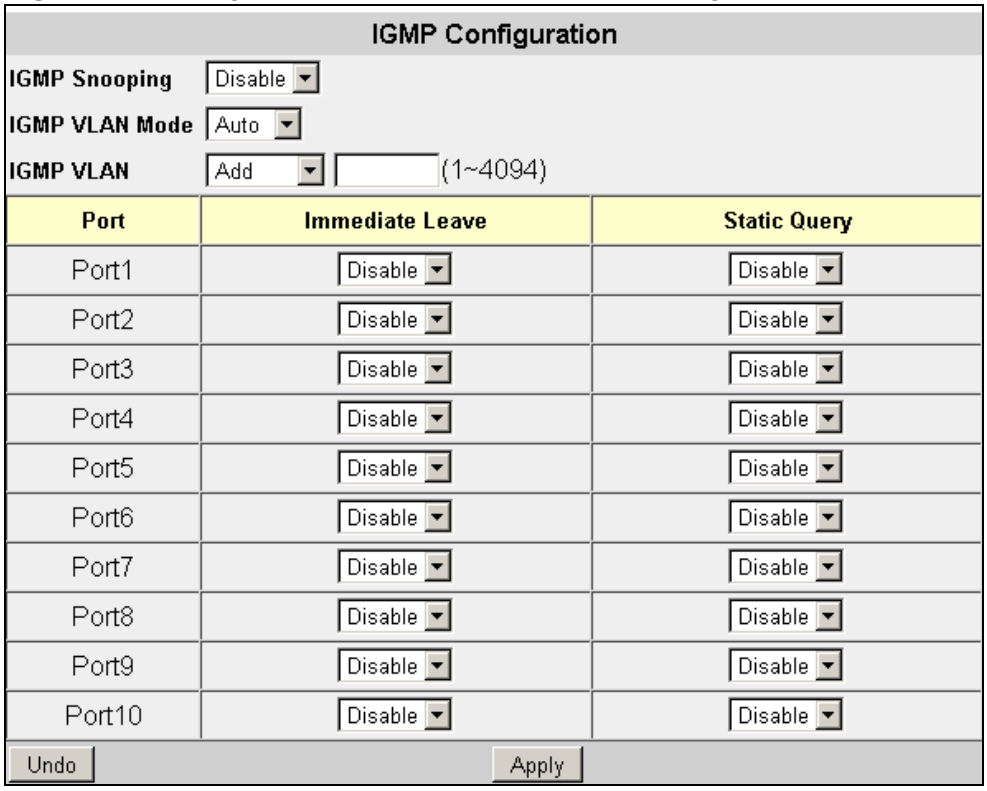
The Switch can perform IGMP snooping on up to 16 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 16 VLANs that send IGMP frames. This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

16.2 IGMP Configuration

Use this screen to configure the Switch's IGMP settings.

Click **Configuration** > **IGMP Menu** > **IGMP Config** to open the following screen.

Figure 53 Configuration > IGMP Menu > IGMP Config



The following table describes the labels in this screen.

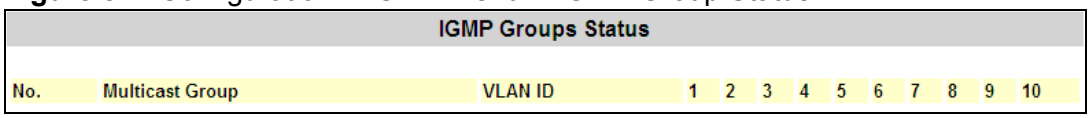
Table 45 Configuration > IGMP Menu > IGMP Config

LABEL	DESCRIPTION
IGMP snooping	Use this to enable or disable IGMP snooping. When IGMP is enabled, the Switch forwards group multicast traffic only to ports that are members of that group.
IGMP VLAN Mode	Select **Auto** to have the Switch learn multicast group membership information of any VLANs automatically. Select **Fixed** to have the Switch only learn multicast group membership information of the VLAN(s) that you specify below.
IGMP VLAN	Enter the ID of the static VLAN(s) that the Switch includes in its learning process of multicast group membership (of the ports). Enter a VLAN ID between 1 and 4094.
Port 1-10	This shows the port numbers that you can configure individually using the fields described below. The Switch can forward multicast frames to IGMP static ports with or without the learning process of multicast group membership.
Immediate Leave	Use this to enable or disable this feature. When Immediate Leave is enabled on this port and the switch receives an IGMP version 2 leave message for this port, this port is immediately removed from the multicast group. When Immediate Leave is disabled on this port and the switch receives an IGMP version 2 leave message for this port, the Switch first uses this port to send a query packet to ask its multicast group if it still has active client requests. After one second and the Switch has not receive a reply packet asking for the port's IGMP report, it removes the port from the multicast group.
Static Query	Select **Enable** to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. Select **Disable** to have the Switch use the port as an IGMP query port if the port receives IGMP query frames.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

16.3 IGMP Status

Click **Configuration > IGMP Menu** > **IGMP Group Status** to display the screen as shown. This screen shows the multicast group information. See Section 16.1 on page 107 for more information on multicasting.

Figure 54 Configuration > IGMP Menu > IGMP Group Status



The following table describes the labels in this screen.

Table 46 Configuration > IGMP Menu > IGMP Group Status

LABEL	DESCRIPTION
No	This is the index number of the entry.
Multicast Group	This field displays IP multicast group addresses.
VLAN ID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.

16.4 MVR Overview

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (**1**, **2** and **3**) information is hidden from the streaming media server, **S**. In addition, the multicast VLAN information is only visible to the Switch and **S**.

Figure 55 MVR Network Example

16.4.1 Types of MVR Ports

In MVR, a source port is a port on the Switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the Switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

16.4.2 MVR Modes

You can set your Switch to operate in either dynamic or compatible mode.

In dynamic mode, the Switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the Switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

16.4.3 How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, **S**, via the Switch. Multiple subscriber devices can connect through a port configured as the receiver on the Switch.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the Switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the Switch, an entry is created in the forwarding table on the Switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the Switch to leave the multicast group. The Switch sends a query to VLAN 1 on the receiver port (in this case, a DSL port on the Switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the Switch removes the receiver port from the forwarding table.

Figure 56 MVR Multicast Television Example

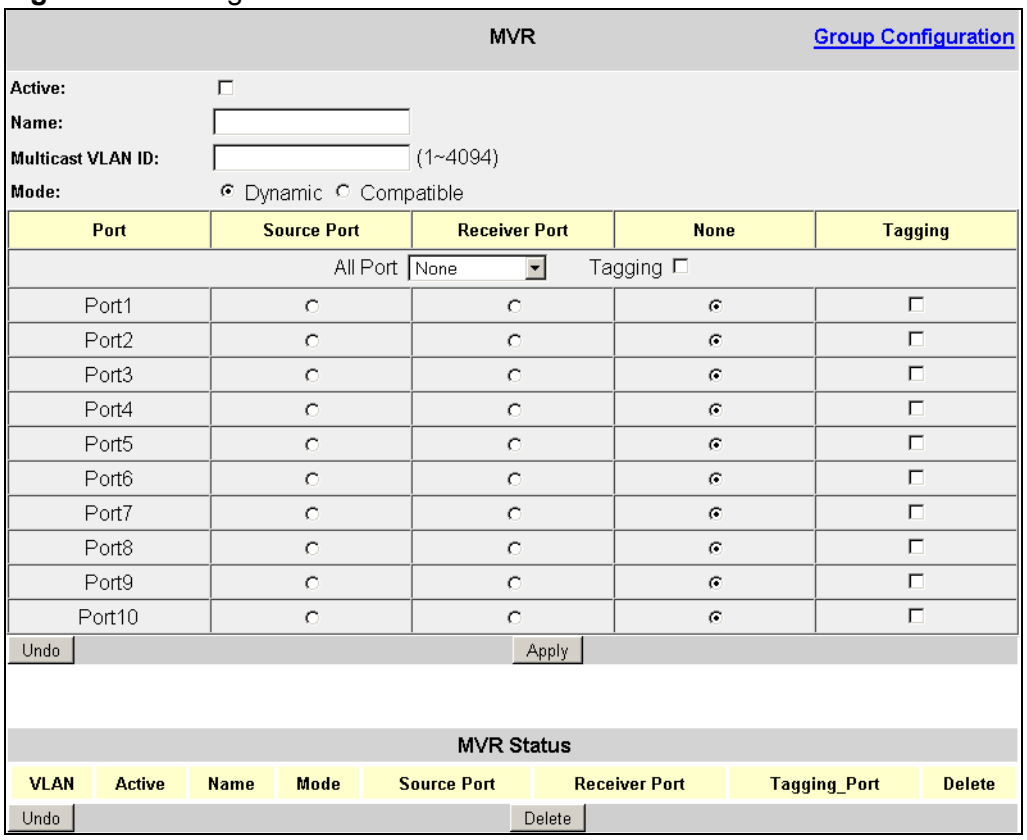
16.5 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Configuration > IGMP Menu** > **MVR** link to display the screen as shown next.

Note: You can create up to three multicast VLANs and up to 256 multicast rules on the Switch.

Note: Your Switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

Figure 57 Configuration > IGMP Menu > MVR



The following table describes the related labels in this screen.

Table 47 Configuration > IGMP Menu > MVR

LABEL	DESCRIPTION
MVR	
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
Mode	Specify the MVR mode on the Switch. Choices are **Dynamic** and **Compatible**. Select **Dynamic** to send IGMP reports to all MVR source ports in the multicast VLAN. Select **Compatible** to set the Switch not to send IGMP reports.
Port	This field displays the port number on the Switch.

Table 47 Configuration > IGMP Menu > MVR (continued)

LABEL	DESCRIPTION
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
All Port	Use this to select between **Source Port**, **Receiver Port** or **None**.
Tagging	Select this checkbox if you want the ports to tag the VLAN ID in all outgoing frames transmitted.
Undo	Click this to load your last saved settings.
Apply	Click this to save your changes.
MVR Status	
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
Tagging Port	This field displays which port tags outgoing frames with the VLAN ID.
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Undo	Click this to clear the **Delete** check boxes.

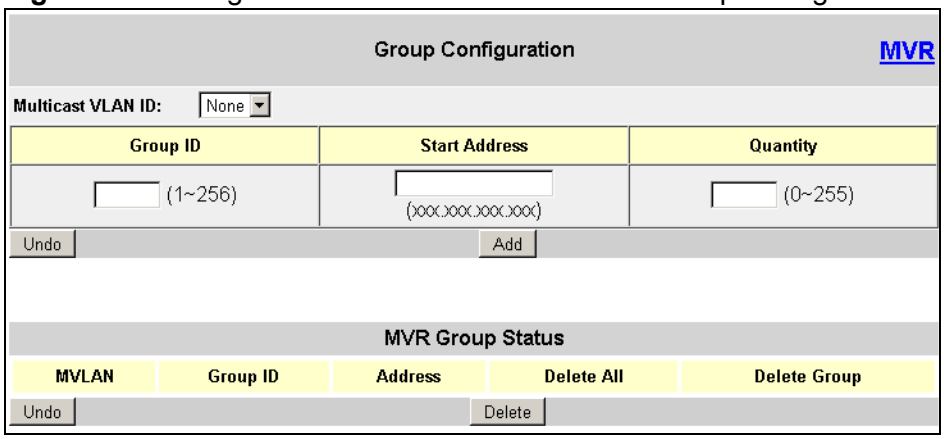
16.6 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Configure MVR IP multicast group address(es) in the **Group Configuration** screen. Click **Group Configuration** in the **MVR** screen.

Note: A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

Figure 58 Configuration > IGMP Menu > MVR > Group Configuration



The following table describes the labels in this screen.

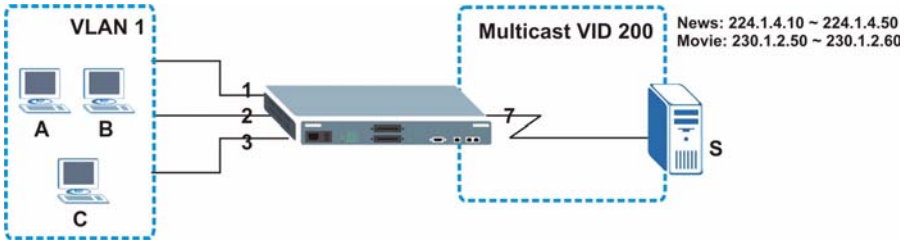
Table 48 Configuration > IGMP Menu > MVR > Group Configuration

LABEL	DESCRIPTION
Group Configuration	
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the **MVR** screen) from the drop-down list box.
Group ID	Enter a group number for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section 16.1.1 on page 107 for more information on IP multicast addresses.
Quantity	Specify the number of IP addresses to include in the multicast group.
Undo	Click this to load your last saved settings.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
MVR Group Status	
MVLAN	This field displays the multicast VLAN ID.
Group ID	This field displays the ID number that identifies the multicast group.
Address	This field displays the starting IP address of the multicast group.
Delet All	Select the check box and click the **Delete** button to remove all configured rules.
Delete Group	Select the check box in the **Delete Group** field and click **Delete** to remove the selected entry(ies) from the table.
Undo	Select this to clear the checkbox(es) in the table.

16.6.1 MVR Configuration Example

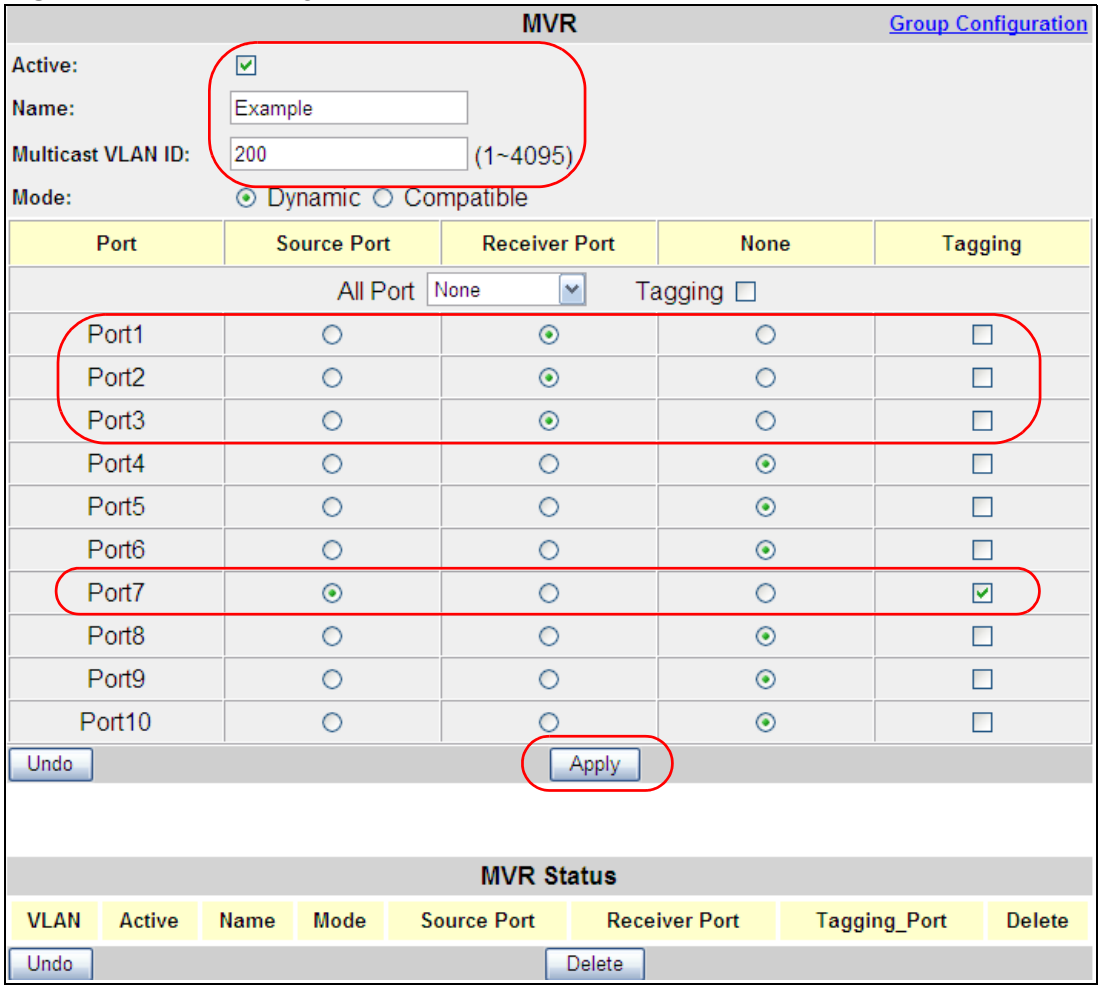
The following figure shows a network example where ports 1, 2 and 3 on the Switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers A, B and C in VLAN are able to receive the traffic.

Figure 59 MVR Configuration Example



To configure the MVR settings on the Switch, create a multicast group in the **MVR** screen and set the receiver and source ports.

Figure 60 MVR Configuration Example



To set the Switch to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The

following figure shows an example where two multicast groups (Group ID **1** for **News** and Group ID **2** for **Movie**) are configured for the multicast VLAN 200.

Figure 61 MVR Group Configuration Example

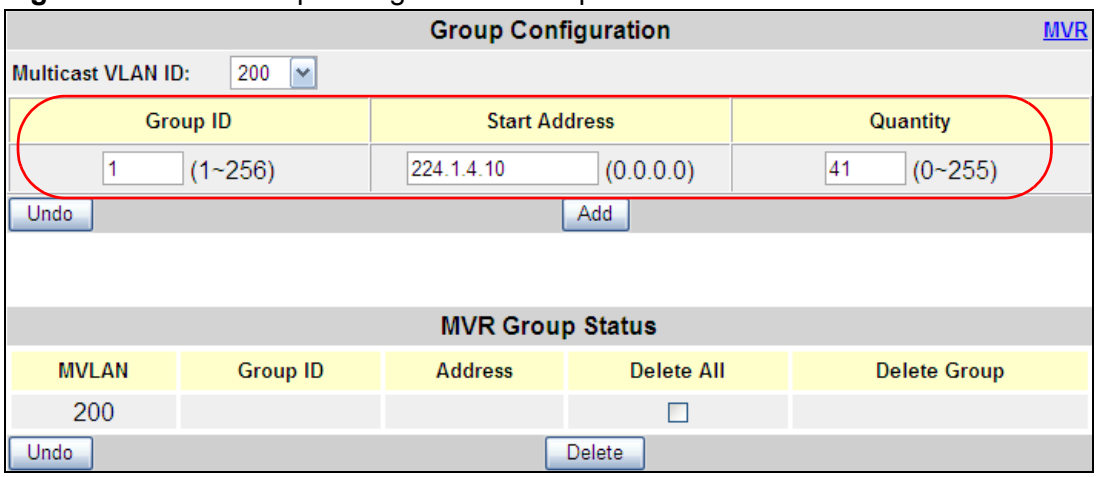
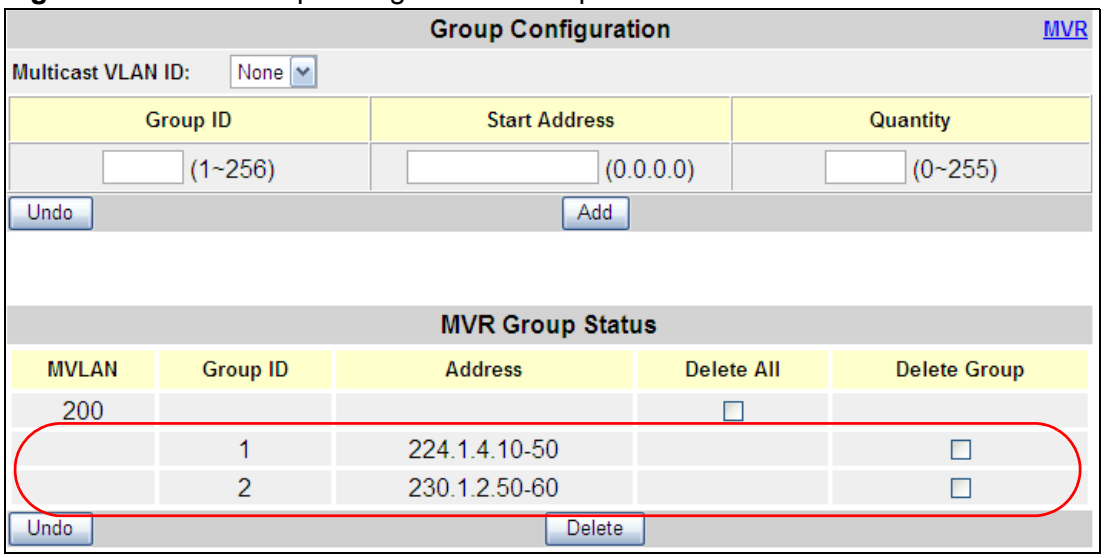


Figure 62 MVR Group Configuration Example



17

IP Source Guard

17.1 Overview

IP source guard uses a binding table to distinguish between authorized and unauthorized DHCP and ARP frames in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

When the Switch receives a DHCP or ARP frame, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Switch forwards the frame. If there is not a binding, the Switch discards the frame.

The Switch builds the binding table by snooping DHCP frames (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP frames on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP frames on the network.

If you want to use dynamic bindings to filter unauthorized ARP frames (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

17.1.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP frames on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

17.1.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP frames that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP frames from trusted ports only if the rate at which DHCP frames arrive is too high. The Switch learns dynamic bindings from trusted ports.

Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.

Untrusted ports are connected to subscribers. The Switch discards DHCP frames from untrusted ports in the following situations:

- The frame is a DHCP server frame (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the frame do not match any of the current bindings.
- The frame is a RELEASE or DECLINE frame, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP frames arrive is too high.

17.1.1.2 DHCP Snooping Static Binding Table

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again. As a result, it is recommended you configure the DHCP snooping database.

17.1.1.3 Configuring DHCP Snooping

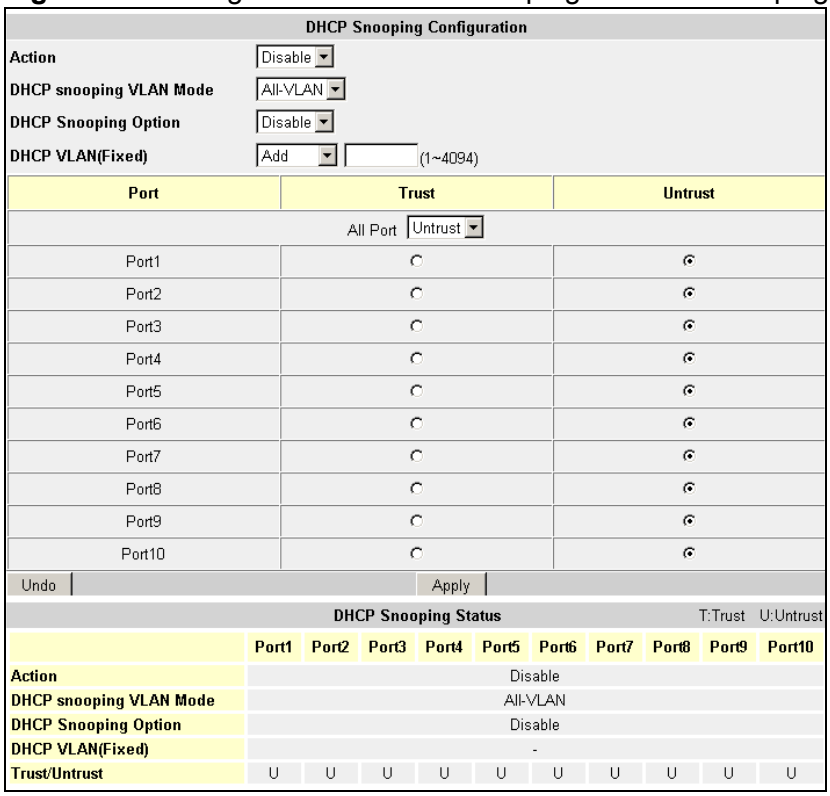
Follow these steps to configure DHCP snooping on the Switch.

1. Enable DHCP snooping on the Switch.
2. Configure trusted and untrusted ports, and specify the maximum number of DHCP frames that each port can receive per second.
3. Configure static bindings.

17.2 DHCP Snooping Configuration

Use this screen to enable DHCP snooping on the Switch and specify whether ports are trusted or untrusted ports for DHCP snooping. To open this screen, click **Configuration > DHCP Snooping > DHCP Snooping Configuration**.

Figure 63 Configuration > DHCP Snooping > DHCP Snooping Configuration



The following table describes the labels in this screen.

Table 49 Configuration > DHCP Snooping > DHCP Snooping Configuration

LABEL	DESCRIPTION
DHCP Snooping Configuration	
Action	Select **Enable** to have the Switch use DHCP snooping . You still have to enable DHCP snooping on specific VLAN and specify trusted ports. Select **Disable** if you do not want to use this feature. Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.
DHCP snooping VLAN Mode	Select **All-VLAN** to have the Switch forward DHCP frames of any VLANs to DHCP servers automatically. Select **Fixed** to have the Switch forward DHCP frames of a specific VLAN to DHCP servers.

Table 49 Configuration > DHCP Snooping > DHCP Snooping Configuration

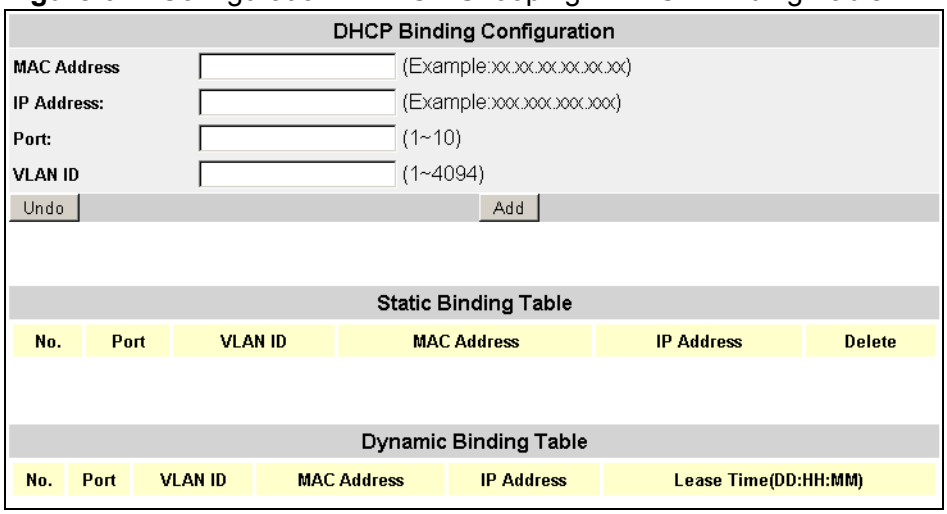
LABEL	DESCRIPTION
DHCP Snooping Option	Select **Enable** to have the Switch add DHCP relay agent option 82 information to DHCP requests that the Switch relays to a DHCP server for each VLAN. Otherwise, select **Disable**.
DHCP VLAN (Fixed)	Enter the ID of a static VLAN; the valid range is between 1 and 4094.
Port	This field displays the port number. If you configure the ***** port, the settings are applied to all of the ports.
Trust	Use this to set trusted ports. Trusted ports are connected to DHCP servers or other switches, and the Switch discards DHCP frames from trusted ports only if the rate at which DHCP frames arrive is too high.
Untrust	Use this to set un-trusted ports. Untrusted ports are connected to subscribers, and the Switch discards DHCP frames from untrusted ports in the following situations: • The frame is a DHCP server frame (for example, OFFER, ACK, or NACK). • The source MAC address and source IP address in the frame do not match any of the current bindings. • The frame is a RELEASE or DECLINE frame, and the source MAC address and source port do not match any of the current bindings. • The rate at which DHCP frames arrive is too high.
All Port	Use this to configure all ports as trusted or un-trusted ports.
Undo	Click this to reset the values in this screen to their last-saved values.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
DHCP Snooping Status	
Action	This shows whether DHCP snooping is enabled or disabled.
DHCP snooping VLAN Mode	This shows whether the Switch forwards DHCP frames of any VLANs or specific VLANs to DHCP servers.
DHCP Snooping Option	This specifies whether or not the Switch enabled or disabled adding DHCP relay agent option 82 information to DHCP requests that the Switch relays to a DHCP server for each VLAN.
DHCP VLAN (Fixed)	This shows the specific VLAN ID.
Trust/Untrust	This shows whether the port is trusted or un-trusted.

17.3 DHCP Binding Table

Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized frames in the network. The Switch learns the bindings by snooping DHCP frames (dynamic bindings) and from information provided manually by administrators (static bindings).

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one. Click **Configuration** > **DHCP Snooping** > **DHCP Binding Table** to open the following screen.

Figure 64 Configuration > DHCP Snooping > DHCP Binding Table



The following table describes the labels in this screen.

Table 50 Configuration > DHCP Snooping > DHCP Binding Table

LABEL	DESCRIPTION
DHCP Binding Configuration	
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
Port	Specify the port in the binding.
VLAN ID	Specify a VLAN ID if you want the Switch to forward DHCP frames to DHCP servers on a specific VLAN. Leave the field blank if you do not want the Switch to forward DHCP frames to a specific VLAN.
Undo	Click this to restore your last saved settings
Add	Click this to add the rule to the Switch.
Static/Dynamic Binding Table	

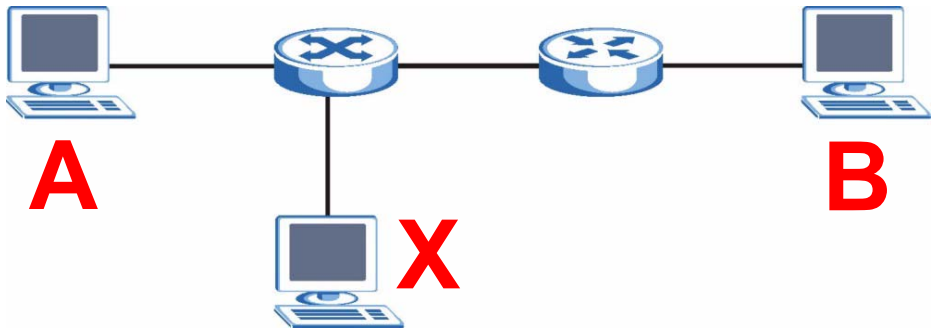
Table 50 Configuration > DHCP Snooping > DHCP Binding Table

LABEL	DESCRIPTION
No.	This field displays a sequential number for each binding.
Port	This field displays the port number in the binding.
VLAN ID	This field displays the source VLAN ID in the binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Delete	Click this to delete a static binding rule.
Lease Time (DD:HH:MM)	This field displays how many days, hours and minutes the binding is valid; for example, **02:03:04** means the binding is still valid for 2 days, 3 hours and 4 minutes.

17.4 The ARP Inspection Screen

Use ARP inspection to filter unauthorized ARP frames on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

Figure 65 Example: Man-in-the-middle Attack



In this example, computer **B** tries to establish a connection with computer **A**. Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A**. Then, computer **X** does the following things:

- It pretends to be computer **A** and responds to computer **B**.
- It pretends to be computer **B** and sends a message to computer **A**.

As a result, all the communication between computer **A** and computer **B** passes through computer **X**. Computer **X** can read and alter the information passed between them.

17.4.1 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

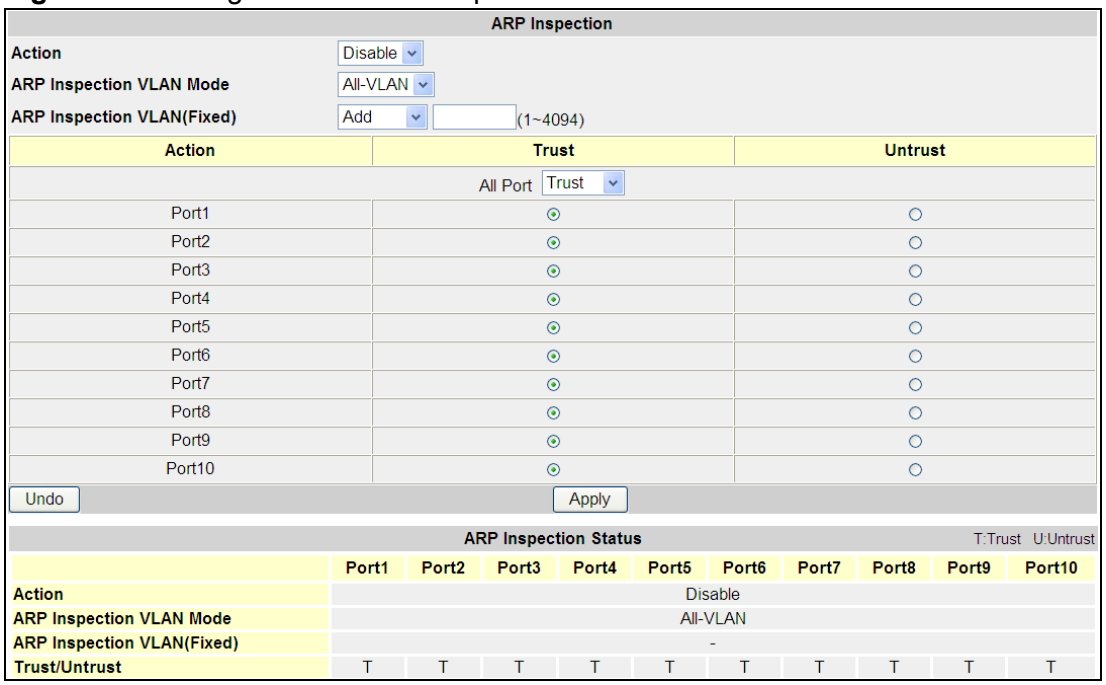
1 Configure DHCP snooping. See Section 17.1.1.3 on page 120.

Note: It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the Switch has enough time to build the binding table.

2 Enable ARP inspection on the Switch. See Section 17.4 on page 124 for more details about turning on this feature.

Click **Configuration** > **ARP Inspection** to open the following screen.

Figure 66 Configuration > ARP Inspection



The following table describes the labels in this screen.

Table 51 Configuration > ARP Inspection

LABEL	DESCRIPTION
ARP Inspection	
Action	Use this to enable or disable the ARP inspection feature.
ARP Inspection VLAN Mode	Select **All-VLAN** to have the Switch look at all the VLANs on which ARP inspection is enabled. Select **Fixed** to have the Switch look at the specific VLANs on which ARP inspection in enabled..

Table 51 Configuration > ARP Inspection

LABEL	DESCRIPTION
ARP Inspection VLAN (Fixed)	Enter the ID of a static VLAN; the valid range is between 1 and 4094.
Action	This is the port number.
Trust	Use this to set trust ports.
Untrust	Use this to set un-trusted ports.
All Port	Use this to configure all ports as trusted or un-trusted ports.
ARP Inspection Status	
Action	This shows whether the ARP inspection feature is enabled or disabled on the Switch.
ARP Inspection VLAN Mode	This shows whether the Switch look at all VLANs or specific VLANs on which ARP inspection in enabled.
ARP Inspection VLAN (Fixed)	This shows the specific VLAN ID.
Trust/Untrust	This shows whether the port is trusted or un-trusted.

18 MAC

18.1 Overview

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

The Switch uses the MAC table to determine how to forward frames. See the following figure.

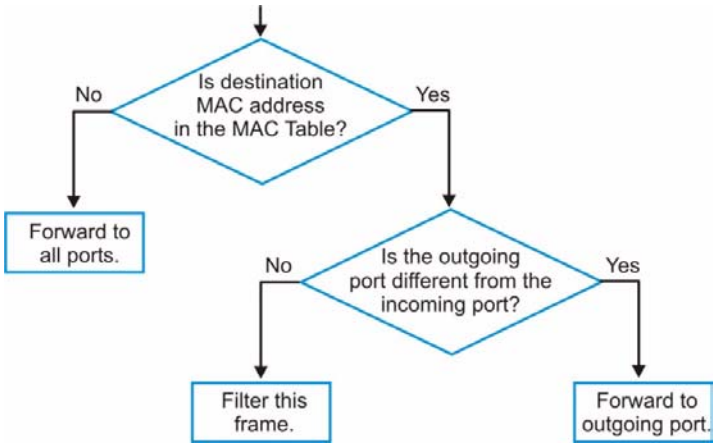
1 The Switch examines a received frame and learns the port on which this source MAC address came.

2 The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.

- If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
- If the Switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.

- If the Switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

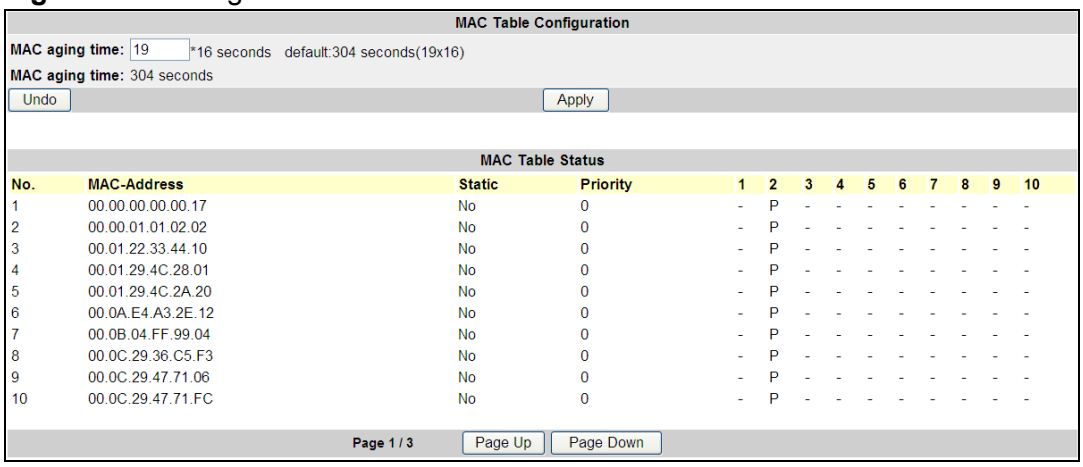
Figure 67 MAC Table Flowchart



18.2 The MAC Table Status Screen

Use this screen to configure the MAC aging time and view the MAC table. Click **Configuration** > **MAC Menu** > **MAC Table Status** to open the following screen.

Figure 68 Configuration > MAC Menu > MAC Table Status


MAC Table Configuration
MAC aging time: 19 *16 seconds default:304 seconds(19x16)
MAC aging time: 304 seconds
Undo
Apply
MAC Table Status
No. MAC-Address Static Priority 1 2 3 4 5 6 7 8 9 10
1 00.00.00.00.00.17 No 0 - P - - - - - - - -
2 00.00.01.01.02.02 No 0 - P - - - - - - - -
3 00.01.22.33.44.10 No 0 - P - - - - - - - -
4 00.01.29.4C.28.01 No 0 - P - - - - - - - -
5 00.01.29.4C.2A.20 No 0 - P - - - - - - - -
6 00.0A.E4.A3.2E.12 No 0 - P - - - - - - - -
7 00.0B.04.FF.99.04 No 0 - P - - - - - - - -
8 00.0C.29.36.C5.F3 No 0 - P - - - - - - - -
9 00.0C.29.47.71.06 No 0 - P - - - - - - - -
10 00.0C.29.47.71.FC No 0 - P - - - - - - - -
Page 1 / 3
Page Up
Page Down

The following table describes the labels in this screen.

Table 52 Configuration > MAC Menu > MAC Table Status

LABEL	DESCRIPTION
MAC Table Configuration	
MAC aging time	Enter a time from 16 to 4080 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
MAC aging time	This is the current MAC aging time.

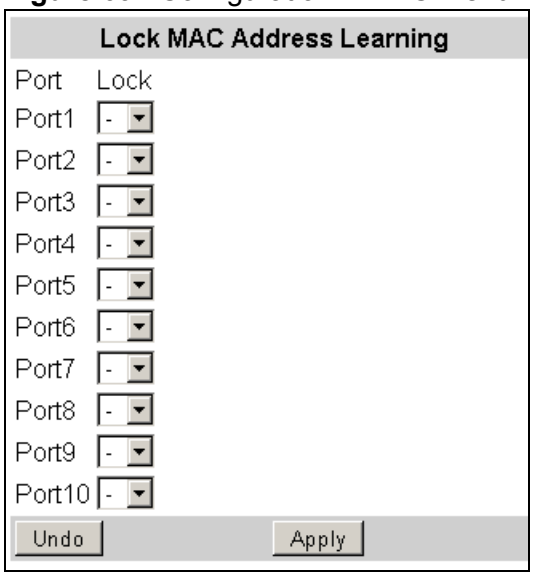
Table 52 Configuration > MAC Menu > MAC Table Status

LABEL	DESCRIPTION
Undo	Click this to load your last saved settings.
Apply	Click this to save your changes.
MAC Table Status	
No.	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
Static	This shows whether the MAC address is dynamic (learned by the Switch) or static (manually configured).
Priority	This shows the priority level of the MAC address
1-10	This shows the port from which the MAC address was learned.
Page Up/Down	Click this to view the previous or next page.

18.3 The Lock MAC Address Learning Screen

Use this screen to configure the MAC address learning settings. Click **Configuration** > **MAC Menu** > **Lock Learning MAC** to open the following screen.

Figure 69 Configuration > MAC Menu > Lock Learning MAC



The following table describes the labels in this screen.

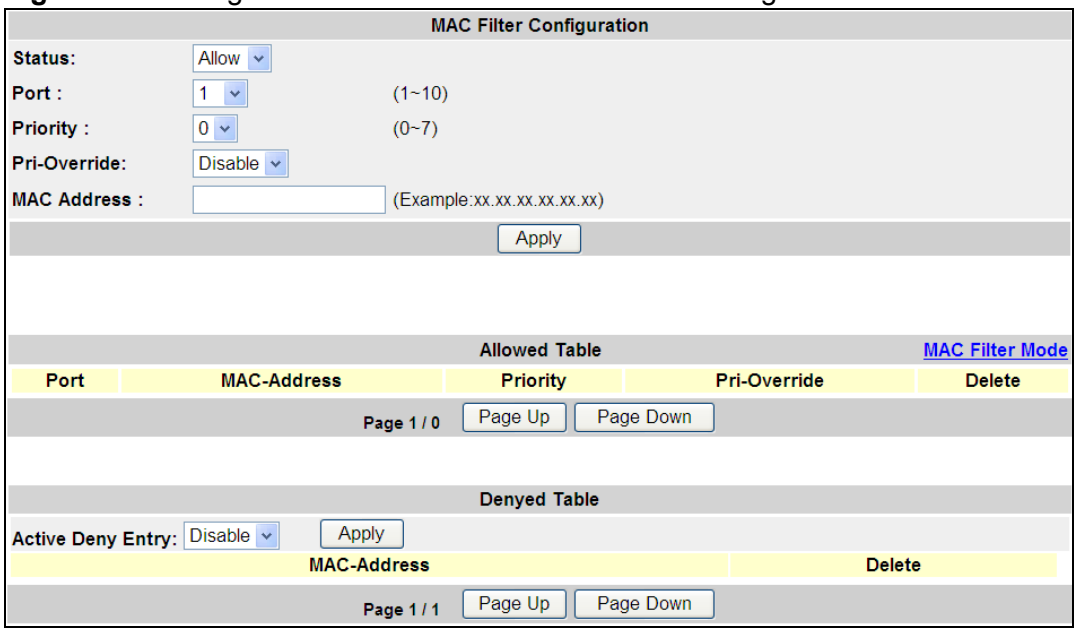
Table 53 Configuration > MAC Menu > Lock Learning MAC

LABEL	DESCRIPTION
Port	This is the port number.
Lock	MAC address learning reduces outgoing broadcast traffic. Use this to activate MAC address learning on the port.
Undo	Click this to load your last saved settings.
Apply	Click this to save your changes.

18.4 The MAC Filter Configuration Screen

Use this screen to configure and view the MAC filter settings. Click **Configuration** > **MAC Menu** > **MAC Filter Config** to open the following screen.

Figure 70 Configuration > MAC Menu > MAC Filter Config



The following table describes the labels in this screen.

Table 54 Configuration > MAC Menu > MAC Filter Config

LABEL	DESCRIPTION
MAC Filter Configuration	
Status	Use this to determine whether to allow or deny traffic transmitted from the source MAC address.
Port	Select the port through which traffic from the source MAC address is transmitted.
Priority	Select a priority level from 0 to 7.

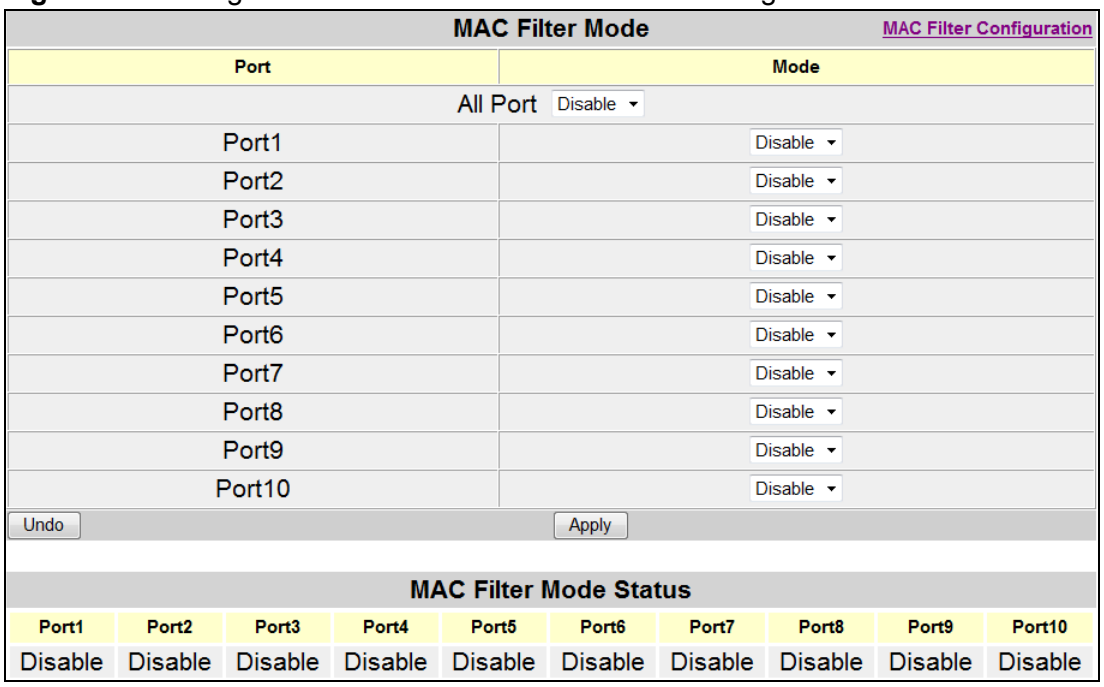
Table 54 Configuration > MAC Menu > MAC Filter Config

LABEL	DESCRIPTION
Pri-Override	Use this to ignore the priority level assigned to the transmitted frames.
MAC Address	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
Apply	Click this to save your changes.
Allowed Table	
Port	This is the port number through which traffic from the source MAC address is transmitted.
MAC Address	This is the source MAC address.
Priority	This shows the priority level.
Pri-Override	This shows whether priority level override is enabled or disabled.
Delete	Click this to remove the rule.
Page Up/Down	Click this to view the previous or next page.
Denied Table	
Active Deny Entry	Use this to enable or disable MAC filtering by denying access from specific MAC addresses.
Apply	Click this to save your changes.
MAC Address	This is the source MAC address.
Delete	Click this to remove the rule.
Page Up/Down	Click this to view the previous or next page.

18.4.1 The MAC Filter Mode Screen

Use this screen to configure the MAC filter setting on each port. In the **Configuration** > **MAC Menu** > **MAC Filter Config** screen, click the MAC Filter Mode link at the top right corner to open the following screen.

Figure 71 Configuration > MAC Menu > MAC Filter Config > MAC Filter Mode



The following table describes the labels in this screen.

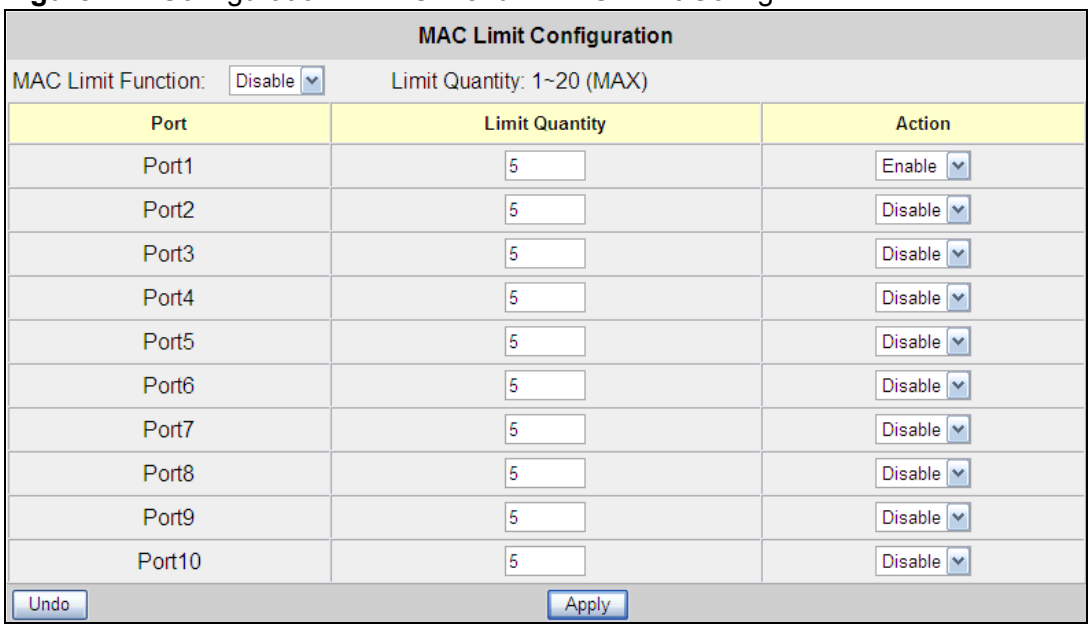
Table 55 Configuration > MAC Menu > MAC Filter Config > MAC Filter Mode

LABEL	DESCRIPTION
MAC Filter Mode	
Port	This identifies the port you are configuring.
Mode	Use this to enable the MAC filter by allow feature on the port. The default setting disables this feature. See Section 18.4 on page 130 for more details about configuring a MAC allow list on each port.
All Port	Use this to apply the setting to all ports.
Undo	Click this to load your last saved settings.
Apply	Click this to save your changes.
MAC Filter Mode Status	
Port1-10	This shows whether the MAC filter by allow feature is enabled or disabled on the port.

18.5 The MAC Limit Configuration Screen

Use this screen to limit the number of MAC addresses that can be learned on a port. Click **Configuration** > **MAC Menu** > **MAC Limit Config** to open the following screen.

Figure 72 Configuration > MAC Menu > MAC Limit Config



The following table describes the labels in this screen.

Table 56 Configuration > MAC Menu > MAC Limit Config

LABEL	DESCRIPTION
MAC Limit Function	Use this to enable or disable the MAC address limit feature.
Port	This is the port number.
Limit Quantity	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the **MAC Table Status** screen.
Action	Enable the MAC limit function on this port. The Switch forwards frames whose MAC address(es) is in the MAC address table on this port. frames with no matching MAC address(es) are dropped. Disable the MAC limit function to forwards all frames on this port.
Undo	Click this to load your last saved settings.
Apply	Click this to save your changes.

19 QoS

19.1 Overview

Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All frames in the flow are given the same priority. You can use QoS to give different priorities to different frame types to solve performance degradation when there is network congestion.

19.2 The QoS Base Configuration Screen

Queuing algorithms allow switches to maintain separate queues for frames from each individual source or flow and prevent a source from monopolizing the bandwidth.

All High Before Low Queuing

All high before low services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

Weighted Round Robin Scheduling (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is a given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

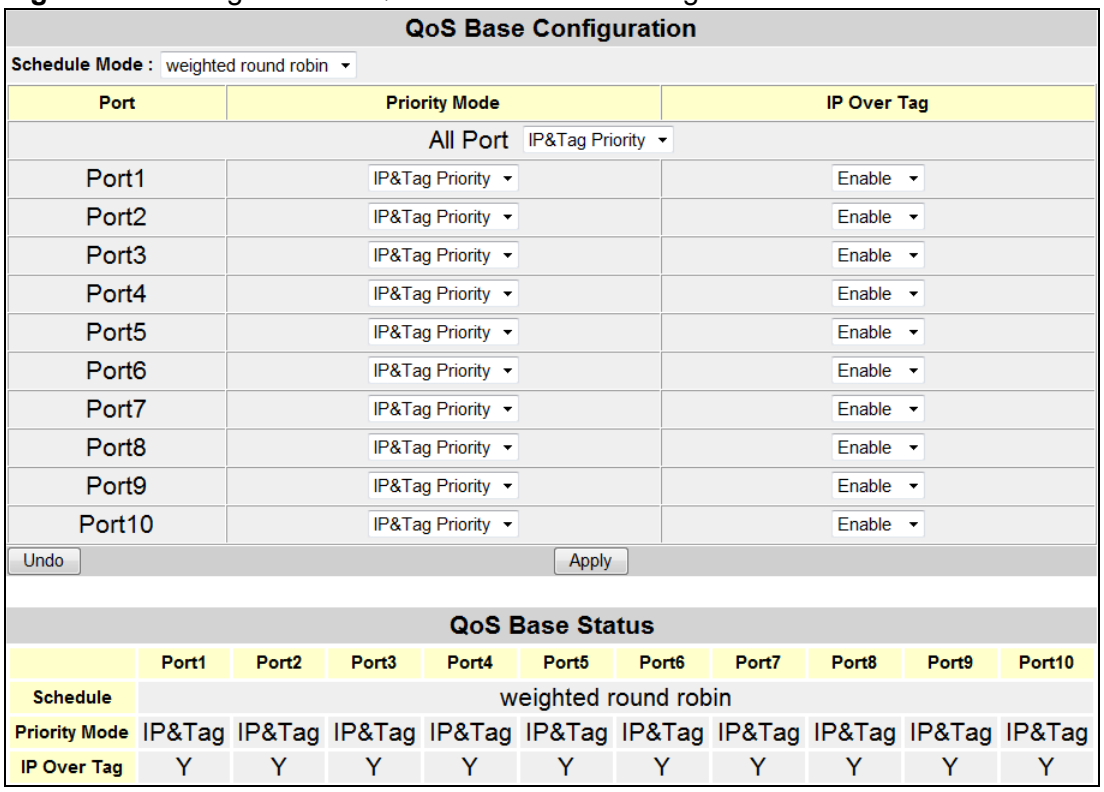
Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can

handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

19.2.1 Configuring the Base Configuration Screen

Use this screen to configure queuing settings on the Switch. Click **Configuration** > **QoS Menu** > **Base Configuration** to open the following screen.

Figure 73 Configuration > QoS Menu > Base Configuration



QoS Base Configuration

Schedule Mode : weighted round robin

Port	Priority Mode	IP Over Tag
All Port	IP&Tag Priority	
Port1	IP&Tag Priority	Enable
Port2	IP&Tag Priority	Enable
Port3	IP&Tag Priority	Enable
Port4	IP&Tag Priority	Enable
Port5	IP&Tag Priority	Enable
Port6	IP&Tag Priority	Enable
Port7	IP&Tag Priority	Enable
Port8	IP&Tag Priority	Enable
Port9	IP&Tag Priority	Enable
Port10	IP&Tag Priority	Enable

Undo Apply

QoS Base Status

	Port1	Port2	Port3	Port4	Port5	Port6	Port7	Port8	Port9	Port10
Schedule	weighted round robin									
Priority Mode	IP&Tag	IP&Tag	IP&Tag	IP&Tag	IP&Tag	IP&Tag	IP&Tag	IP&Tag	IP&Tag	IP&Tag
IP Over Tag	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

The following table describes the labels in this screen.

Table 57 Configuration > QoS Menu > Base Configuration

LABEL	DESCRIPTION
QoS Base Configuration	
Schedule Mode	Select **all high before low** or **weighted round robin**. All high before low queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight. Queues with larger weights get more service than queues with smaller weights.
Port	This label shows the port you are configuring.

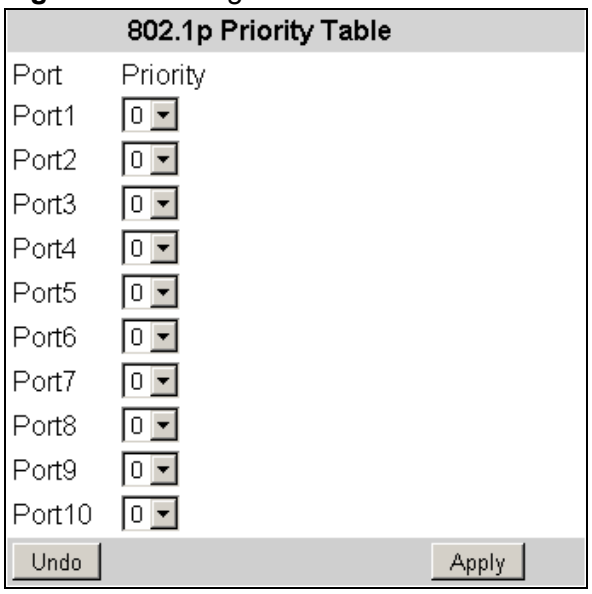
Table 57 Configuration > QoS Menu > Base Configuration

LABEL	DESCRIPTION
Priority Mode	Select a priority mode for the port. **802.1p Priority** uses port priority as queuing basis. Assign a priority level to each port in the **802.1p Priority** screen (Section 19.3 on page 138). **Tag Priority** uses VLAN tag priority as queuing basis. See Section 19.4 on page 139 for more details on configuring tag priority. **IP ToS Priority** uses IP DSCP priority as queuing basis. See Section 19.5 on page 139 for more details on configuring IP DSCP priority. **IP & Tag Priority** uses both IP DSCP priority and tag priority as queuing basis.
IP Over Tag	Use this to enable or disable IP Over Tag on the port. When you enable this feature and the Switch receives a frame containing both IP DSCP and tag priority information, the Switch will only use the IP DSCP priority information.
All Port	Use this to set the priority mode for all ports.
Undo	Click this to load your last saved settings.
Apply	Click this to save your changes.
QoS Base Status	
Port1-10	This is the port number.
Schedule	This is the schedule mode used on the Switch.
Priority Mode	This is the priority mode used on the port.
IP Over Tag	This shows whether the IP over tag feature is enabled or disabled on the Switch.

19.3 The 802.1p Priority Table

Use this screen to assign a priority level for each port. Click **Configuration** > **QoS Menu** > **802.1p Priority** to open the following screen.

Figure 74 Configuration > QoS Menu > 802.1p Priority



The following table describes the labels in this screen.

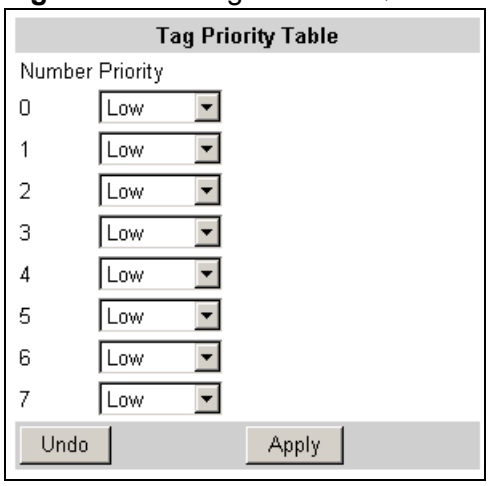
Table 58 Configuration > QoS Menu > 802.1p Priority

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
Priority	Assign a priority level to the port.
Undo	Click this to load your last saved settings.
Apply	Click this to save your changes.

19.4 The Tag Priority Table

Click **Configuration** > **QoS Menu** > **Tag Priority** to open the following screen.

Figure 75 Configuration > QoS Menu > Tag Priority



The following table describes the labels in this screen.

Table 59 Configuration > QoS Menu > Tag Priority

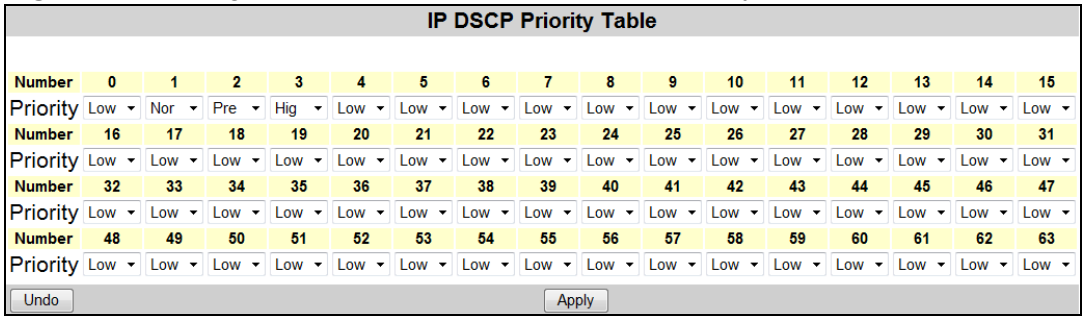
LABEL	DESCRIPTION
Number	This is the IEEE 802.1p priority level.
Priority	Use this to assign the tag priority level to one of the Switch's queue level (**Low**, **Normal**, **Preferred** or **High**).
Undo	Click this to load your last saved settings.
Apply	Click this to save your changes.

19.5 The IP DSCP Priority Table

DiffServ is a class of service (CoS) model that marks frames so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Frames are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the frames differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

Use this to assign DSCP priority settings. Click **Configuration** > **QoS Menu** > **IP DSCP Priority** to open the following screen.

Figure 76 Configuration > QoS Menu > IP DSCP Priority


IP DSCP Priority Table
Number 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Priority Low Nor Pre Hig Low Low Low Low Low Low Low Low Low Low Low Low
Number 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Priority Low Low Low Low Low Low Low Low Low Low Low Low Low Low Low Low
Number 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
Priority Low Low Low Low Low Low Low Low Low Low Low Low Low Low Low Low
Number 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
Priority Low Low Low Low Low Low Low Low Low Low Low Low Low Low Low Low
Undo
Apply

The following table describes the labels in this screen.

Table 60 Configuration > QoS Menu > IP DSCP Priority

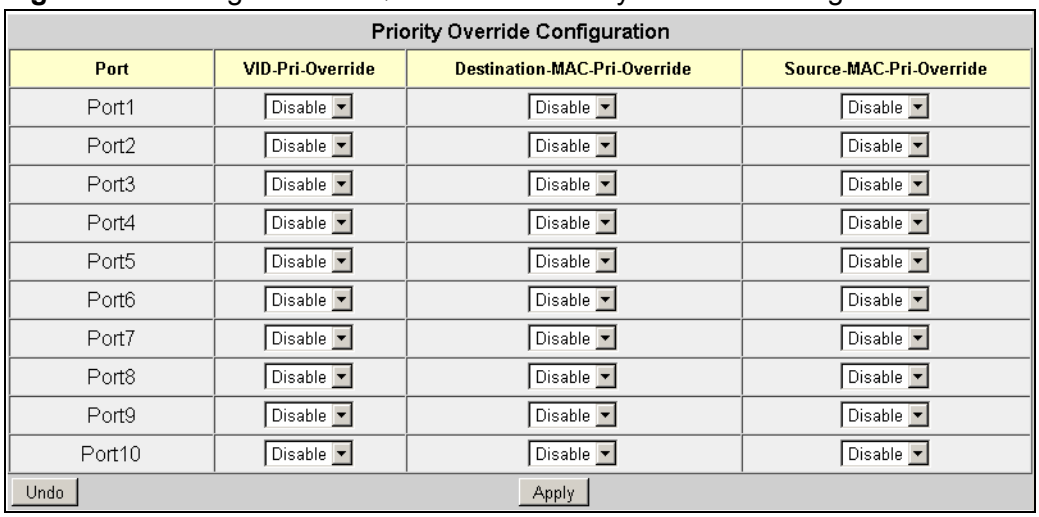
LABEL	DESCRIPTION
Number	This is the DSCP classification identification number.
Priority	Assign a Switch's priority level (**Low**, **Normal**, **Preferred** or **High**) to the DSCP value.
Undo	Click this to load your last saved settings.
Apply	Click this to save your changes.

19.6 The Priority Override Configuration Screen

Use this screen to apply the QoS settings of the Switch to its DHCP clients. The Switch ignores the priority levels assigned to the transmitted frames on the ports, source MAC addresses and destination MAC addresses.

Click **Configuration** > **QoS Menu** > **Priority Override Configuration** to open the following screen.

Figure 77 Configuration > QoS Menu > Priority Override Configuration



The following table describes the labels in this screen.

Table 61 Configuration > QoS Menu > Priority Override Configuration

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
VID-Pri-Override	Select **Enable** to have the Switch ignore the priority level assigned to the transmitted frames on this port. Select **Disable** if you do not want to use this feature. This is selected by default.
Destination-MAC-Pri-Override	Select **Enable** to have the Switch ignore the priority level assigned to the transmitted frames on the destination MAC address. Select **Disable** if you do not want to use this feature. This is selected by default.
Source-MAC-Pri-Override	Select **Enable** to have the Switch ignore the priority level assigned to the transmitted frames on the source MAC address. Select **Disable** if you do not want to use this feature. This is selected by default.
Undo	Click this to load your last saved settings.
Apply	Click this to save your changes.

PART IV
Management

Mgmt Config and System Restart Menu
(145)

20

Mgmt Config and System Restart Menu

20.1 Overview

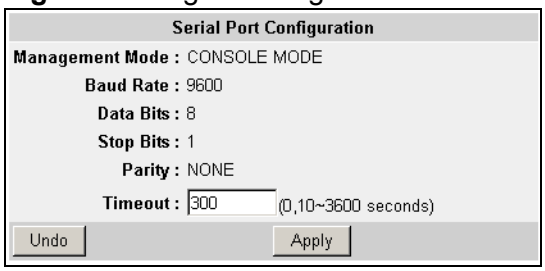
This chapter explains how to configure the screens that let you maintain the firmware and configuration files.

20.2 The Serial Port Configuration Screen

Use this screen to view the parameters for local management. Configure a computer's terminal emulation software with the displayed parameters to manage the Switch. Connect the male 9-pin end of the console cable to the console port of the Switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

Click **Mgmt Config** > **Serial Port Config** to open the following screen.

Figure 78 Mgmt Config > Serial Port Config

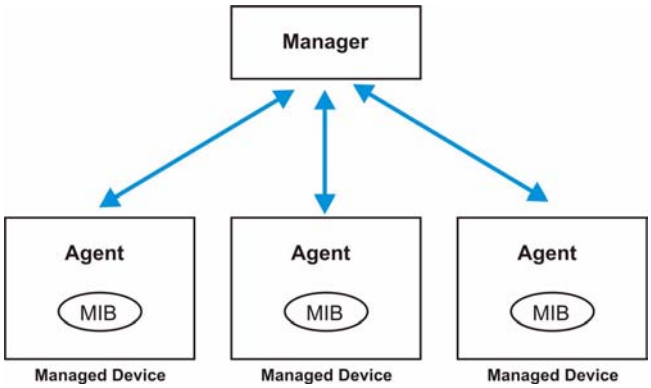


Specify the amount of time (in seconds) before the console session disconnects automatically. If you set the timeout to 0 second, the console session never expires. Click **Apply** to save your changes.

20.3 The SNMP Configuration Screens

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network via SNMP version one (SNMPv1), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 79 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (the Switch). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

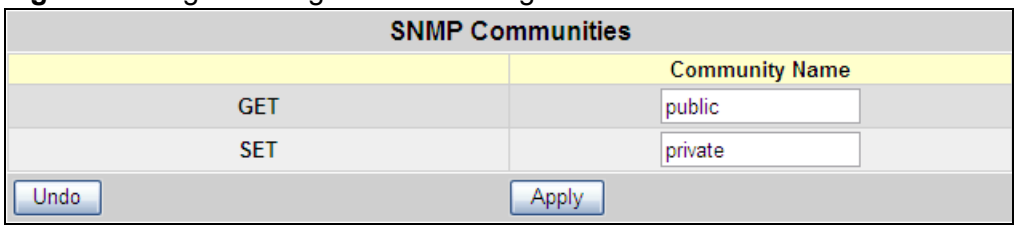
Table 62 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

20.3.1 The SNMP Communities Screen

Use this screen to configure the SNMP communities. Click **Mgmt Config** > **SNMP Config** > **SNMP Communities** to open the following screen.

Figure 80 Mgmt Config > SNMP Config > SNMP Communities



The following table describes the labels in this screen.

Table 63 Mgmt Config > SNMP Config > SNMP Communities

LABEL	DESCRIPTION
GET	Enter the Get community string, which is the password for the incoming Get- and GetNext- requests from the management station.
SET	Enter the Set community string, which is the password for incoming Set- requests from the management station.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

20.3.2 The IP Trap Manager Screen

An IP trap manager receives authentication failure messages or other trap messages about the Switch's activities. The Switch supports up to five trap

managers. Use this screen to configure the trap manager settings. Click **Mgmt Config** > **SNMP Config** > **IP Trap Manager** to open the following screen.

Figure 81 Mgmt Config > SNMP Config > IP Trap Manager

The following table describes the labels in this screen.

Table 64 Mgmt Config > SNMP Config > IP Trap Manager

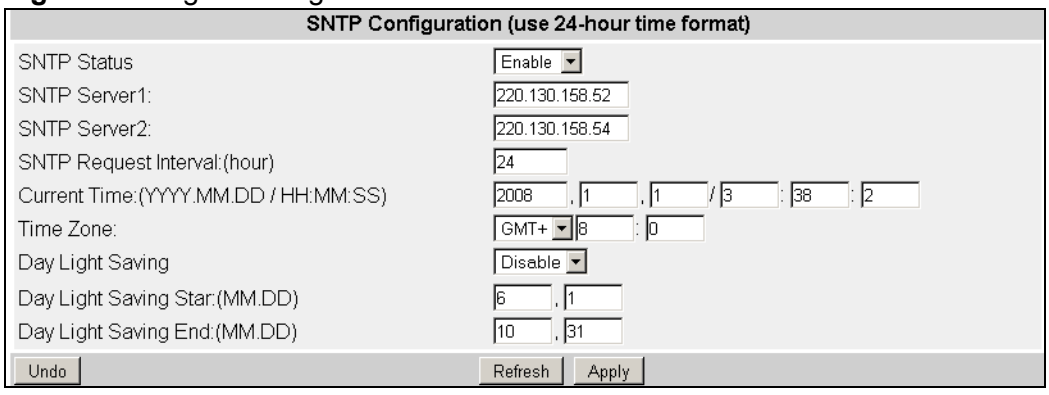
LABEL	DESCRIPTION
IP Address	Enter the IP addresses of up to five managers to send your SNMP traps to.
Community Name	Enter the community string.
Status	Use this to enable or disable the trap manager feature.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

20.4 The SNTP Screen

Use this screen to configure the time settings on the Switch. You can configure the Switch to get the time and date information from a time server using Simple Network Time Protocol (SNTP). You can also configure two servers. If the first one is down, the Switch will try to connect to the second one.

Click **Mgmt Config** > **SNTP** to open the following screen.

Figure 82 Mgmt Config > SNTP



The following table describes the labels in this screen.

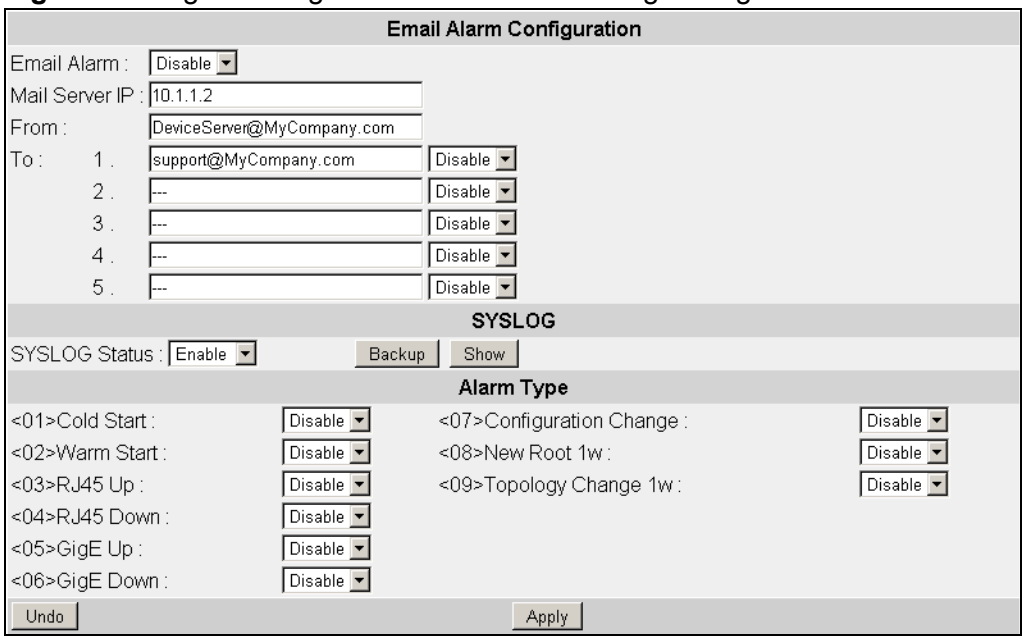
Table 65 Mgmt Config > SNTP

LABEL	DESCRIPTION
SNTP Status	Use this to enable or disable time server for the Switch.
SNTP Server 1 and 2	Enter the IP address of your time server.
SNTP Request Interval	Specify how often (in hours) should the Switch synchronize with the time server. For example, if you set the field to 2 hours, the Switch synchronizes date/time with the time server every 2hours.
Current Time	Specify the date (in year, month and day format) and time (in hour, minute and second format).
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone.
Day Light Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Enable this option if you use Daylight Saving Time.
Day Light Saving Start	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Saving Time**. The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. You'll have to manually configure the date every year as the date changes every year.
Day Light Saving End	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Saving Time**. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. You'll have to manually configure the date every year as the date changes every year.
Undo	Click this to restore your last saved settings.
Refresh	Click this to reset the data for the field(s).
Apply	Click this to save your changes.

20.5 Alarms and Logs

Use this screen to configure the mail server, the syslog and alarm settings. Click **Mgmt Config** > **Email Alarm & SYSLog Config** to open the following screen.

Figure 83 Mgmt Config > Email Alarm & SYSLog Config



The following table describes the labels in this screen.

Table 66 Mgmt Config > Email Alarm & SYSLog Config

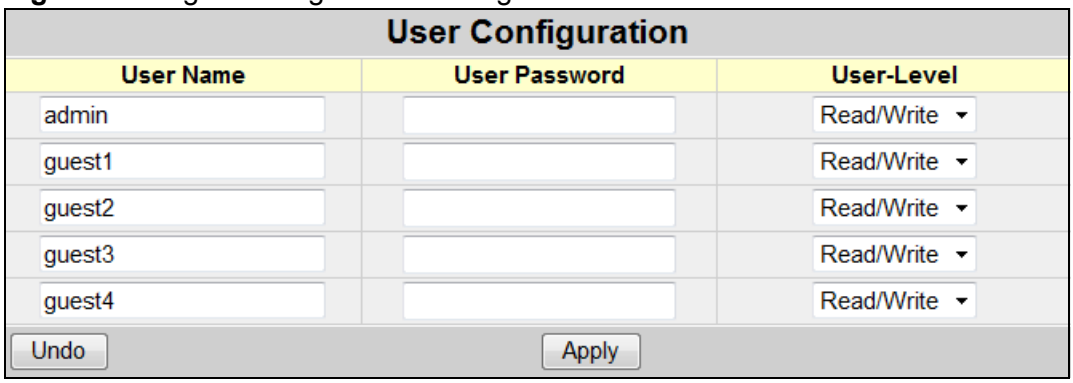
LABEL	DESCRIPTION
Email Alarm Configuration	
Email Alarm	Use this to enable or disable the e-mail alarm system.
Mail Server IP	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alerts messages will not be sent via e-mail.
From	Assign a valid e-mail address to the Switch.
To	The Switch sends logs to the e-mail addresses specified in this field. If this field is left blank, the Switch does not send logs via e-mail.
SYSLOG	
SYSLOG Status	Use this to enable or disable syslog logging.
Backup	Click this save syslog file to a TFTP server.
Show	Click this to show a complete list of syslog messages.
Alarm Type	Select the categories of alarm that you want to record and send an e-mail alarm.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

20.6 The User Configuration Screen

Use this screen to configure user names, passwords and access right for up to five user accounts. Click Mgmt Config > User Config to open the following screen.

Note: It is recommended that only one user log in and manage the device at a time. When multiple users configure the device settings simultaneously, changes may be overwritten.

Figure 84 Mgmt Config > User Config



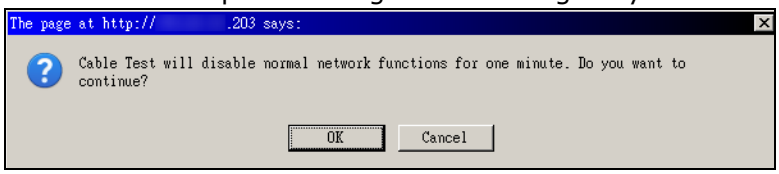
The following table describes the labels in this screen.

Table 67 Mgmt Config > User Config

LABEL	DESCRIPTION
User Name	Enter a name to identify the user account. You can type up to 15 characters using characters found on a standard keyboard.
User Password	Enter a password associated with the user name. You can type up to 15 characters using characters found on a standard keyboard.
User-Level	Assign access rights for the user account. **Read/Write** users can manage the Switch settings as an administrator. **Read Only** users can only view the Switch settings.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

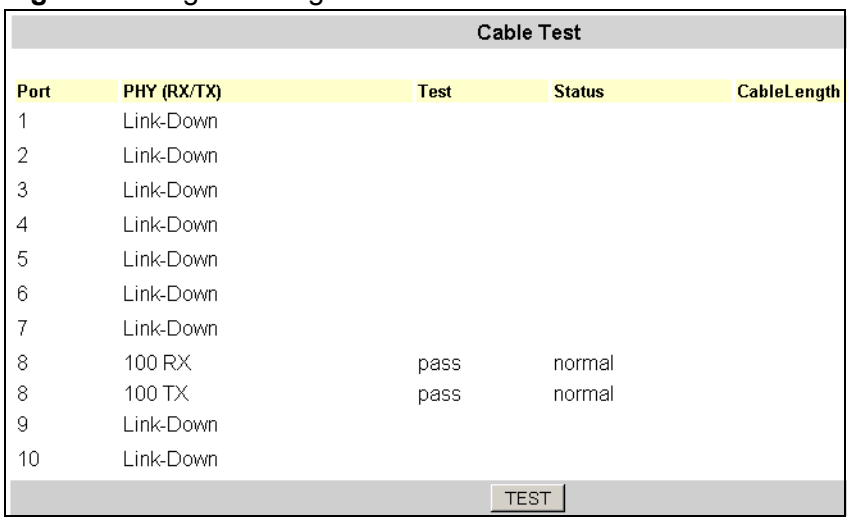
20.7 The Cable Test Screen

Use this feature to diagnose the connection on each port. Click **Mgmt Config** > **Cable Test** to open a dialogue box asking for your confirmation.


The page at http:// .203 says:
Cable Test will disable normal network functions for one minute. Do you want to continue?
OK
Cancel

Click **OK** to start the test. The test results are shown as follows.

Figure 85 Mgmt Config > Host Denial-of-Service Protection



The following table describes the labels in this screen.

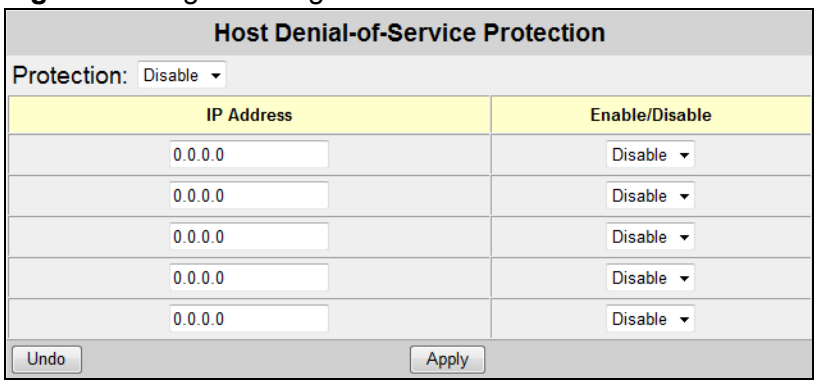
Table 68 Mgmt Config > Host Denial-of-Service Protection

LABEL	DESCRIPTION
Port	This is the port number.
PHY (RX/TX)	This shows if data is flowing through the ports on the Switch. If no data is passing through a port, this shows **Link-Down**. Otherwise, the number indicates the maximum size of packets during data transmission in the port.
Test	If the cable is well connected to the port, this shows **Pass**. Otherise, this shows **Fail**.
Status	If the cable is well connected to the port, this is **Normal**. If the connection is down, you see an **Open** status.
CableLength	This shows the length of the cable connected to the port.
TEST	Click this to run the test again.

20.8 The Host DoS Protection

You can specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch. When you turn on this feature, only the trusted IP addresses listed in this screen can use remote management to access the Switch. Click **Mgmt Config** > **Host Denial-of-Service Protection** to open the following screen.

Figure 86 Mgmt Config > Host Denial-of-Service Protection



The following table describes the labels in this screen.

Table 69 Mgmt Config > Host Denial-of-Service Protection

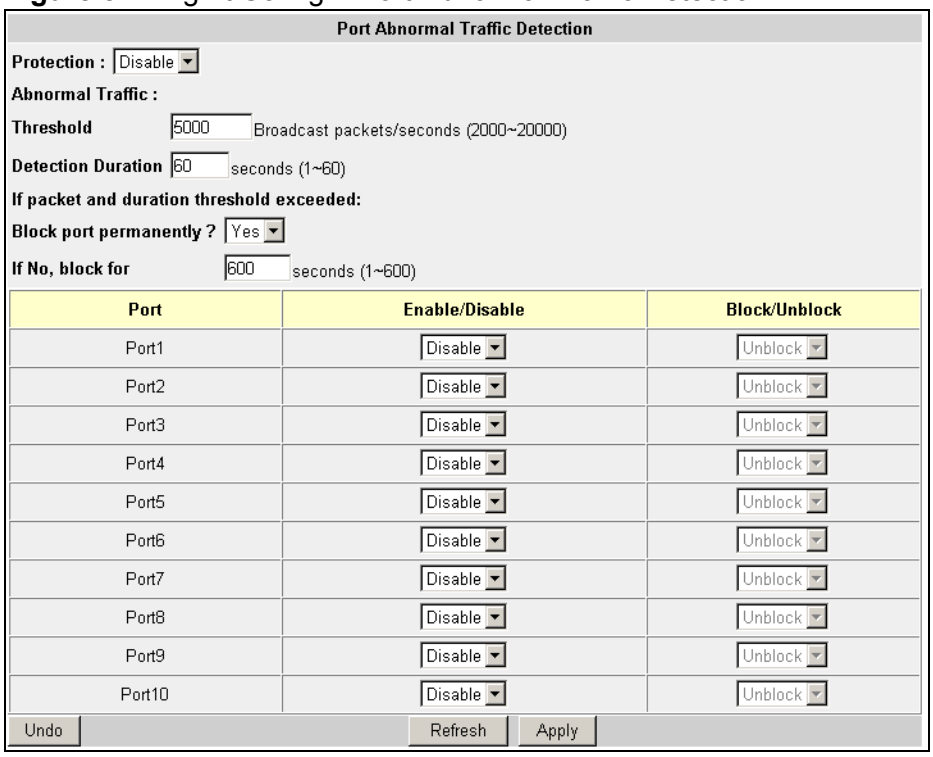
LABEL	DESCRIPTION
Protection	Use this to enable or disable host denial-of-service protection.
IP Address	Configure the IP address of the trusted computer from which you can manage this Switch. The Switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The Switch immediately disconnects the session if it does not match.
Enable/Disable	Select **Enable** to activate this secured client set. Select **Disable** if you wish to temporarily disable the set without deleting it.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

20.9 The Port Abnormal Traffic Detection Screen

This Switch can detect excessive broadcasts or transmission load on a port and temporarily or permanently block traffic transmission on each port. Use this screen to configure the Switch's threshold settings for blocking a port. You can also have the Switch unblock a port when it is no longer receiving large broadcast packets.

Click **Mgmt Config** > **Port Abnormal Traffic Detection** to open the following screen.

Figure 87 Mgmt Config > Port Abnormal Traffic Detection



The following table describes the labels in this screen.

Table 70 Mgmt Config > Port Abnormal Traffic Detection

LABEL	DESCRIPTION
Protection	Use this to enable or disable abnormal traffic detection on the Switch.
Abnormal Traffic	Set the rules for abnormal traffic in the fields described below.
Threshold	Specify a threshold value (in broadcast packets per second). If transmission load on a port exceeds this threshold, the Switch blocks the port. The block can be blocked permanently or for a period of time, depending on what you specify in this screen (see fields below).

Table 70 Mgmt Config > Port Abnormal Traffic Detection

LABEL	DESCRIPTION
Detection Duration	Specify for how long (up to 60 seconds) the threshold is exceeded before the Switch blocks the port. This allows the port(s) to exceed the threshold for a short time period depending on the number of seconds you specify. The port is blocked when the transmission load continues and the number of seconds has expired.
If packet and duration threshold exceeded	
Block port permanently	Select **Yes** to block the port for good if traffic exceeds the threshold for a certain time. You can manually unblock a port in the **Block/Unblock** field. However the port is only unblocked when it is not receiving excessive traffic anymore.
If No, block for N seconds	Specify for how long the Switch will block the port if traffic exceeds the threshold.
Port	This shows the port number(s) that you can configure.
Enable/Disable	If you enabled abnormal traffic detection on the Switch, use this to enable or disable abnormal traffic detection on a specific port. The rules you set will only apply to ports that are set to **Enable**.
Block/Unblock	Use this field to manually block or unblock a port. Select **Block** to have the Switch block a port according to the abnormal traffic detection values you specified in this screen. Select **Unblock** to have the Switch unblock a previously blocked port when it is not receiving abnormal traffic anymore.
Undo	Click this to restore your last saved settings.
Apply	Click this to save your changes.

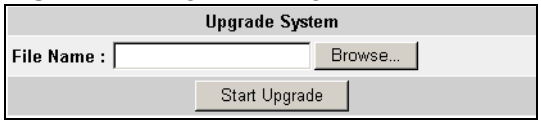
20.10 Upgrading the Firmware

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

Click **Mgmt Config** > **Firmware Download** to open the following screen.

Figure 88 Mgmt Config > Firmware Download



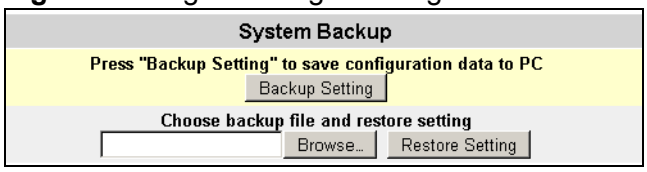
Type the path and file name of the firmware file you wish to upload to the Switch in the **File Name** field or click **Browse** to locate it. Click **Start Upgrade** to load the new firmware.

After the firmware upgrade process is complete, the device will automatically restart. See the **System Details** > **Board Info.** screen to verify your current firmware version number.

20.11 Managing the Configuration File

Backing up your Switch configurations allows you to create various "snap shots" of your device from which you may restore at a later date. Use this screen to back up or restore a configuration file. Click **Mgmt Config** > **Configuration File** to open the following screen.

Figure 89 Mgmt Config > Configuration File



Follow the steps below to back up the current Switch configuration to your computer in this screen.

1 Click **Backup Setting**.

2 Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

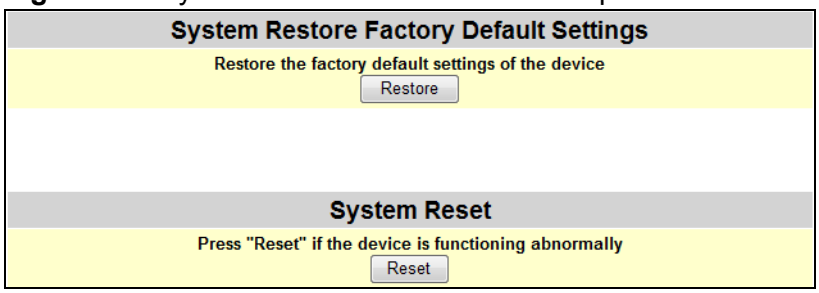
To restore a configuration file, type the path and file name of the configuration file you wish to restore in the field or click **Browse** to locate it. After you have specified the file, click **Restore Setting**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

20.12 Restarting the System

Click **System Restart Menu** > **Restart Option** to open the following screen. Use the Restore button to load the factory default settings, or use the Reset button to

restart the system without physically turning the power off. It also allows you to load the factory default settings when you reboot.

Figure 90 System Restart Menu > Restart Option


System Restore Factory Default Settings
Restore the factory default settings of the device
Restore
System Reset
Press "Reset" if the device is functioning abnormally
Reset

PART V
Troubleshooting & Product Specifications

Troubleshooting (161)

Product Specifications (165)

21

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Switch Access and Login

21.1 Power, Hardware Connections, and LEDs

The Switch does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the Switch.
2. Make sure the power adaptor or cord is connected to the Switch and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the Switch.
4. If the problem continues, contact the vendor.

The **ALM** LED is on.

1. Disconnect and re-connect the power adaptor or cord to the Switch.
2. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Section 3.2 on page 34.

2 Check the hardware connections. See Section 21.1 on page 161.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Disconnect and re-connect the power adaptor or cord to the Switch.

5 If the problem continues, contact the vendor.

21.2 Switch Access and Login

I forgot the IP address for the Switch.

1 The default IP address is **192.168.1.1**.

2 Use the console port to log in to the Switch.

3 If this does not work, you have to reset the device to its factory defaults. See Section 4.6 on page 45.

I forgot the username and/or password.

1 The default username is **admin** and the default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 4.6 on page 45.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address, use the new IP address.

- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Switch.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 3.2 on page 34.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 Make sure your computer is in the same subnet as the Switch. (If you know that there are routers between your computer and the Switch, skip this step.)

5 Reset the device to its factory defaults, and try to access the Switch with the default IP address. See Section 4.6 on page 45.

6 If the problem continues, contact the vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Switch using another service, such as Telnet. If you can access the Switch, check the remote management settings to find out why the Switch does not respond to HTTP.

I can see the **Login** screen, but I cannot log in to the Switch.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.

Check that you have enabled logins for HTTP or Telnet. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.

3 Disconnect and re-connect the cord to the Switch.

4 If this does not work, you have to reset the device to its factory defaults. See Section 4.6 on page 45.

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

22

Product Specifications

The following tables summarize the Switch's hardware and firmware features.

Table 71 Hardware Specifications

SPECIFICATION	DESCRIPTION
Dimensions	268 mm (W) x 128 mm (D) x 44 mm (H)
Weight	1.2 kg
Power Specification	AC: 110-240V AC, 50/60 Hz, 14 W Max.
Interfaces	8 10/100 Base-Tx ports 2 GbE Dual Personality interfaces (Each interface has one 1000Base-T RJ-45 port and one Small Form-Factor Pluggable (SFP) slot, with one port active at a time.) 2 mini-GBIC (SFP) slots Auto-negotiation Auto-MDIX One console port Compliant with IEEE 802.3/3u Back pressure flow control for half duplex Flow control for full duplex (IEEE 802.3x)
LEDs	Per switch: PWR, SYS Per Fast Ethernet RJ-45 10/100 port: LNK/ACT Per mini-GBIC slot: LNK, ACT Per mini-GBIC slot (in dual personality interface): LNK/ACT
Operating Environment	Temperature: 0º C ~ 50º C Humidity: 10 ~ 95% (non-condensing)
Storage Environment	Temperature: -40º C ~ 70º C Humidity: 10 ~ 95% (non-condensing)

Table 72 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Administrator User Name	admin
Default Password	1234
Number of Login Accounts Configurable on the Switch	5 accounts configured on the Switch.
VLAN	A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.
VLAN Stacking	Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.
MAC Address Filter	Filter traffic based on the source and/or destination MAC address.
IGMP Snooping	The Switch supports IGMP snooping, enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your Switch.
QoS	Queuing is used to help solve performance degradation when there is network congestion. The following scheduling services are supported: weighted round robin and all high before low queuing. This allows the Switch to maintain separate queues for frames from each individual source or flow and prevent a source from monopolizing the bandwidth.
Bandwidth Control	Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.
Broadcast Storm Control	The device supports per port TCP/IP ingress rate limiting along with independent storm prevention.
Port Mirroring	Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.

Table 72 Firmware Specifications

FEATURE	DESCRIPTION
Multicast VLAN Registration (MVR)	Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across a network. MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.
L2 Multicast	The device supports Layer-2 multicast switching with line-rate (wire speed) switching for all packet sizes and conditions. In addition, the Switch can send packets to Ethernet devices that are not VLAN-aware by untagging (removing the VLAN tags) IP multicast packets.
STP (Spanning Tree Protocol)	STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.
Loop Detection	Use the loop detection feature to monitor any network loops on the edge of your network.
IP Source Guard	Use IP source guard to filter unauthorized DHCP and ARP packets in your network.
Link Aggregation	Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.
Port Authentication and Security	For security, the Switch allows authentication using IEEE 802.1x with an external RADIUS server and port security that allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch.
Authentication and Accounting	The Switch supports authentication and accounting services via RADIUS.
Device Management	Use the web configurator or commands to easily configure the rich range of features on the Switch.
Syslog	The Switch can generate syslog messages for system monitoring.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, CLI or TFTP tool to put it on the Switch. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the Switch's configuration and put it back on the Switch later if you decide you want to revert back to an earlier configuration.

The following list, which is not exhaustive, illustrates the standards supported in the Switch.

Table 73 Standards Supported

STANDARD	DESCRIPTION
RFC 826	Address Resolution Protocol (ARP)
RFC 894	Ethernet II Encapsulation
RFC 1112	IGMP v1
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1213	SNMP MIB II
RFC 1493	Bridge MIBs
RFC 1643	Ethernet MIBs
RFC 1757	RMON
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2138	RADIUS (Remote Authentication Dial In User Service)
RFC 2139	RADIUS Accounting
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 3046	DHCP Relay
RFC 4330	Simple Network Time Protocol(SNTP)
IEEE 802.1x	Port Based Network Access Control
IEEE 802.1D	MAC Bridges
IEEE 802.1p	Traffic Types - Packet Priority
IEEE 802.1Q	Tagged VLAN
IEEE 802.1w	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.3	Packet Format
IEEE 802.3ad	Link Aggregation
IEEE 802.3x	Flow Control
Safety	UL 60950-1 CSA 60950-1 EN 60950-1 IEC 60950-1
EMC	FCC Part 15 (Class A) CE EMC (Class A)

PART VI
Appendices and Index

Changing a Fuse (171)

Common Services (173)

Legal Information (177)

Index (181)

A

Changing a Fuse

This appendix shows you how to remove and install fuses for the Switch.

If you use a fuse other than an included fuse, make sure it matches the fuse specifications in the appendix on product specifications.

Removing a Fuse

Disconnect all power from the Switch before you begin this procedure.

1. Remove the power cord from the Switch.
2. See the product specifications for the location of the fuse. Use a small flat-head screwdriver to carefully pry out the fuse housing.
3. A burnt-out fuse is blackened, darkened or cloudy inside its glass casing. A working fuse has a completely clear glass casing. Pull gently, but firmly, to remove the burnt out fuse from the fuse housing. Dispose of the burnt-out fuse properly.

Installing a Fuse

1. The Switch is shipped from the factory with one spare fuse included in a box-like section of the fuse housing. Push the middle part of the box-like section to access the spare fuse. Put another spare fuse in its place in order to always have one on hand.
2. Push the replacement fuse into the fuse housing until you hear a click.
3. Push the fuse housing back into the Switch until you hear a click.
4. Plug the power cord back into the unit.

B

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s**) is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 74 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.

Table 74 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).

Table 74 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

C

Legal Information

Copyright

Copyright © 2009 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.

- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index

A

abnormal traffic detection 154
accounts 151
alarms 150
application
  backbone 19
  bridging 20
  metropolitan 22
  trunking 21
  VLAN 21
ARP inspection 119, 124
auto negotiation 54

B

backbone application 19
bandwidth control 95
BPDU 76
bridge 75
  BPDU 76
  configuration 78
  path cost 75, 79
  port states 77
  priority 79
Bridge Protocol Data Unit, see BPDU
bridging application 20
broadcast 107
broadcast storm control 97

C

configuration
  bandwidth control 95
  bridge 75, 78
  broadcast storm control 97
  date/time 148
  DHCP snooping 121
  IGMP 109
  jumbo frames 63
  link aggregation 103
  loop detection 59
  MAC filtering 130
  multicast 109
  MVR 112
  port mirroring 99
  ports 53
  QoS 136
  trunking 103
  VLAN 85
configuration file 156
connection test 152
console port 30, 145

D

date/time 148
DHCP binding 123
DHCP client 48, 49
DHCP snooping 119, 120, 121
DoS 153
duplex 54

E

external authentication server 71

F

firmware upgrade 155
flow control 55
forward delay 79
forwarding frames 84
front panel 29

G

Gigabit Ethernet ports 30

H

hardware
  console port 30
  front panel 29
  Gigabit Ethernet ports 30
  installation 25
  LEDs 34
  mini-GBIC slots 31
hash mode 104
Hello Time 79

I

IEEE 802.1x
  port authentication 65
IGMP 107
  configuration 109
  snooping 107
installing hardware 25
IP address 48
IP DSCP priority 139
IP source guard 119
  ARP inspection 124
  configuration 121
  DHCP snooping 120

J

jumbo frames 63

L

LEDs 34
link aggregation 101
  configuration 103
  dynamic 101
  hash mode 104
  ID 102
  static 102
  status 105
  system priority 105
lockout 45
login 37
logs 150
loop detection 59

M

MAC filtering 127
  configuration 130
  MAC learning 129
management 145
  abnormal traffic detection 154
  alarms 150
  configuration file 156
  connection test 152
  console port 30, 145
  date/time 148
  DoS 153
  firmware upgrade 155
  logs 150
  reset 156
  SNMP 146
  user accounts 151
  web configurator 37
management VLAN 94
max age 79
metropolitan application 22
mini-GBIC slots 31
multicast 107
  configuration 109, 112
  IGMP snooping 107
  MVR 110
Multicast VLAN Registration, see MVR
MVR 110
  configuration 112

N

naming the system 48

navigation panel 40

P

password 44
path cost 75, 79
port authentication
  and RADIUS 71
port configuration 53
port mirroring 99
port-based VLANs 85
priority mode, QoS 137

Q

QoS 135
  configuration 136
  IP DSCP priority 139
  port priority 138
  priority mode 137
  tag priority 139

R

RADIUS 71
  advantages 71
  and port authentication 71
  server 71
Rapid Spanning Tree Protocol, see RSTP
reset 45, 156
RMON status 57
RSTP 75
  BPDU 76
  bridge priority 79
  configuration 78
  path cost 75, 79
  port states 77

S

SNMP 146
SNTP 148
stacking, VLAN 91
stacking, VLANs 87
static bindings 119
status
  IGMP 110
  link aggregation 105
  MAC filtering 128
  multicast 110
  ports 55
  RMON 57
  trunking 105
switch lockout 45
system
  abnormal traffic detection 154
  configuration file 156
  connection test 152
  DHCP client 48, 49
  firmware upgrade 155
  information 47
  IP address 48
  lockout 45
  login 37
  logs 150
  name 48
  password 44
  reset 45, 156
  user accounts 151

T

TACACS+ 71
Tag Protocol Identifier, see TPID
tag-based VLANs 91
tagged VLANs 83
time/date 148
TPID 89
trunking 101
  application 21
  configuration 103
  dynamic 101
  hash mode 104
  ID 102
  static 102
  status 105
  system priority 105

U

unicast 107
user accounts 151

V

VLAN 83
  application 21
  configuration 85
  forwarding frames 84
  frame formats 90
  management VLAN 94
  port-based 85
  stacking 87, 91
  tag format 89
  tag-based 91
  tagged 83

W

web configurator 37
  navigation panel 40
weighted round robin scheduling 135